Mainframe Computing Environments

Security Assessment Guide

August 19, 2002

Final

Prepared by:
Barre Bull, Project Manager
Gay Macaranas, IT Security Analyst

13921 Park Center Road, Suite 300,
Herndon, VA 20171

SAIC-6663-2002-108

Prepared for:
Mr. Greg Montgomery
U.S. Department of Agriculture
Room 431-W
Whitten Building
14th and Independence
Washington, D.C. 20250

For Official Use Only

U.S. Department of Agriculture

Washington, D.C. 20250

USDA Mainframe Computing Environment Security Assessment Guide

1. PURPOSE

This Security Assessment Guide is designed to assist Agency ISSPMs in satisfying their responsibility to develop and implement a comprehensive risk management program as defined in DR 3140-001, "USDA Information Systems Security Policy." By using this guide, Agency ISSPMs can identify areas where Department Information Security requirements are not being met and develop an action plan to ensure all security requirements are satisfied.

2. SCOPE

This guide is to be used by all USDA organizational elements to help assess the security posture of Mainframe Computing Environment. This checklist is ***not intended to be a configuration guide*** but a tool to assist in determining if the system meets the requirements for a Sensitive But Unclassified (SBU) system and assessing the vulnerabilities, both current and potential, of the system. The checks performed are based on Federal, USDA, and Best Security Practices for the protection of SBU data. This checklist does not address applications installed on the system or special purpose configurations (i.e. web servers, database servers, etc.).

3. BACKGROUND

Risk Assessments are mandated by OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources." A security risk assessment process is a comprehensive evaluation of the system's technical and non-technical security features. It establishes the extent that a specific design and implementation meets specific security requirements.

4. REFERENCES

a. External

(1) Public Law 100-235, "Computer Security Act of 1987"
(2) Public Law 93-579, "Privacy Act of 1974"
(3) Public Law 93-502, "Freedom of Information Act"
(4) Public Law 99-474, "Computer Fraud and Abuse Act"
(5) OMB Circular No. A-130 Appendix III, "Security of Federal Automated Information Resources," revised February 8, 1996.
(6) OMB Circular No. A-123, "Management Accountability and Control," June 29, 1995.

b. USDA Internal Regulations

(1) DR 3140-001, “USDA Information Systems Security Policy” dated May 15, 1996.

(2) DM 3140-1 “USDA Management ADP Security Manual” dated March 5, 1992.

Mainframe Computing Environment Assessment Guide

This assessment should be completed by the Agency's ISSPM or designated alternate in conjunction with the Agency Assessment Checklist. Answer all questions. Provide supplemental information as appropriate. All "No" or "Partial" answers must include supplemental information (such as the given reason why the requirement cannot be met) and an action plan that describes how the requirement will be met, as well as a schedule for completion of the plan. Typically, this would be achieved by developing the action plan in this document and reflecting this in the security plan for the agency.

Agency Identification:

Agency (Agency, Office, Bureau, Service, etc.):		
Address		
CIO		Phone:
ISSPM		Phone:
Date of last Assessment:		

Test Number: **1**	SITE:	DATE:	TIME:
Test Name: **SYSTEM INTEGRITY**			
Resources Required:	Mainframe Terminal Access		
Personnel Required:	Systems Programmer / Security Administrator		
Objectives:	Review the system resources and support structures.		
Procedure Description: (Summary)	Verify that the system resources and support structures are configured and functioning properly.		

Detailed Procedures and Results

Step #	Procedure Description SYSTEM INTEGRITY	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
	System Authorization Facility (SAF) Configuration The System Authorization Facility (SAF) provides an installation with centralized control over system security processing through a system service called the OS/390 router.			
1.	Is the SAF interface or equivalent used as an interface across products and platforms?	Products and platforms that utilize SAF as an interface can be protected with the security software such as CA-ACF2, RACF, CA-Top Secret		
2.	Do all data sets supporting the system resources and security software have restricted authority?	Only authorized personnel who require the authority to modify or maintain the security software and system resources should have change/modify access.		
3.	Are Commercial-Off -The-Shelf (COTS) products and associated datasets within the operating system using the security software?	Ensure that all COTS products on the operating system utilize the SAF interface or equivalent to the security software.		
4.	Are Government-Off the Shelf (GOTS) products along with associated data sets using the security software?	Whenever possible, Government-Off the Shelf (GOTS) products should be using the SAF interface or equivalent. Safeguards enforced by the security software should not be duplicated by security mechanisms implemented within an application. Limit developed internal security mechanisms to those functions that augment the safeguards present in the security software.		
5.	Are newly developed applications, along with associated data sets using the security software?	Whenever possible, newly developed applications should be using the SAF interface or equivalent. Limit developed internal security mechanisms to those functions that augment the safeguards present in the security software.		

Step #	Procedure Description SYSTEM INTEGRITY	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
6.	Are the internal security controls for the COTS or GOTS products only used when existing products or applications cannot interface with the security software through SAF?	Only use the internal security controls for the COTS or GOTS products when existing products or applications do not interface to the security software through SAF.		
	Software Development and Test Domains It is important to ensure that the software development and test domains for the operating system, and the security software are protected from internal and external attacks.			
7.	Is testing of new or modified software performed in a specific or isolated environment?	Testing of new or modified software should be performed in a specific or isolated environment.		
8.	Is the security software installed and configured in the test or development domains to be fully compliant to the organization?	Changes to the system software and configuration, including the security systems, should be tested in a LPAR separate and unique from the production LPAR(s).		
9.	Are the development and test domains network connections severed or disabled from the production systems?	The development and test domains network connections should be severed or disabled from the production systems.		
10.	Are special privileges only granted to authorized personnel for a specific period of time or duration of the test?	Special privileges should only be limited or restricted to authorized personnel for a specific period of time or the duration of the test.		
	HARDWARE INTEGRITY If configured or handled improperly, hardware components can create exposures within the operating environment that cannot be controlled with any software process.			
11.	**Direct Access Storage Devices (DASD)** Is access to DASD resources defined and restricted with the security software?	Access to the DASD resources should be defined and restricted with the security software.		
12.	**Tapes** Is access to Tape resources defined and restricted with the security software?	Access to the Tape resources should be defined and restricted with the security software.		
13.	**System Consoles** Is access to Console resources defined and restricted with the security software?	Access to System Console resources defined and restricted with the security software.		
14.	Are master consoles defined as remote access consoles?	Master consoles should not be defined as remote access consoles.		
15.	Are physical access control mechanisms for the hardware environment designed and implemented as part of the physical security plan?	Physical access control mechanisms for the hardware environment should be designed and implemented as part of the physical security plan.		
16.	Are the hardware components of the Front End Processors (FEPs) in a secure location?	The hardware components of the Front End Processors (FEPs) should be in a secure location.		

Step #	Procedure Description SYSTEM INTEGRITY	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
17.	Are only authorized users allowed access to and use of the facilities where the Front End Processors (FEPs) are located?	Physical security is critical for the protection of the control panel, the operator console (local and/or remote), and the diskette drive of the service subsystem. Only authorized users should be allowed access to and use of those facilities.		
	SOFTWARE INTEGRITY If configured or handled improperly, software components can create exposures within the operating environment.			
	System Change Control Any modification or upgrades to the system software and security software			
18.	Is there a change control process for software changes / modifications?	There should be a change control process for software changes / modifications.		
19.	Are change control mechanisms strictly enforced for QA and Production?	Change control mechanisms should be strictly enforced QA and Production.		
20.	Is the IBM's System Modification Program/Extended (SMP/E) utilized to install and maintain all products?	Install and maintain all products with the capability for installation via IBM's System Modification Program / Extended (SMP/E). This will ensure proper control and tracking of maintenance and changes for the system.		
21.	Are all products (HW/SW/FW) tested in a test environment for security impacts before being authorized for the production system?	All products (HW/SW/FW) should be tested in a test environment before being authorized for the production system.		
22.	Operator Over-rides Is there an automated process for IPL's and started procedures?	There should be an automated process for IPL's and started procedures.		
	Authorized Program Facility (APF) APF is a component of the OS/390 that allows installations to specify programs permitted to use sensitive system functions.			
23.	Are the APF libraries change / modify authorities restricted to authorized personnel only?	APF libraries change / modify authorities should be restricted to authorized personnel only?		
24.	Are activities on the APF-authorized libraries logged and monitored routinely?	Activities on the APF-authorized libraries should be logged and monitored routinely.		
	TSO APF Authorization Allows Time Sharing Option (TSO) users to execute authorized programs.			
25.	Are programs requiring TSO authorization reviewed for potential impacts to the operating system?	Programs that require TSO authorization should be reviewed for potential impacts to the operating system.		

Step #	Procedure Description SYSTEM INTEGRITY	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
	Program Properties Table (PPT) Programs in the PPT can bypass security software mechanisms such as password protection			
26.	Are the programs defined in the PPT tables reviewed routinely to ensure that only programs that require special authorizations are coded in the PPT?	Only programs that require special authorization should be coded in the PPT.		
27.	Are the programs defined by IBM and vendors documented?	The programs defined by IBM and vendors should be documented.		
28.	Are the systems operating defaults and additions documented?	The system operating defaults and additions should be documented.		
	Supervisor Calls (SVC) An SVC is a low-level language instruction that initiates an operating system interrupt. The operating system passes control to the SVC code to perform processing. All SVC code runs in Supervisor State, which means that SVC code can potentially violate system integrity.			
29.	Are SVCs provided by third party or written locally evaluated for potential abuse, validity checking and protection of the system?	SVCs provided by third party or written locally should be evaluated for it's potential abuse, validity checking, and protection of the system.		
	I/O Appendages An I/O appendage is a routine that provides additional control over system I/O operations. An I/O appendage can examine the status of I/O operations and determine the actions to be taken for various conditions. Appendages have the potential to circumvent or disable security software files, to modify audit trails, or to modify other data.			
30.	Are I/O appendages defined to the system evaluated for their potential exposure to the system?	I/O appendages defined to the system should be evaluated for their potential exposure to the system.		
	OS/390 and Other Products Such as the security software, SMF, JES2, TSO, ISPF, CICS, OMEGAMON, and SDSF System products provide exits that can be used to perform additional process for an installation. These exits have the potential to open the integrity exposures since the code may be entered in an authorized state.			
31.	Are exits that are vendor supplied or locally written reviewed and validated so that the code does not bypass the integrity of the operating environment?	Every exit that is vendor supplied or locally written should be validated so the code does not bypass the integrity of the operating environment.		
	Link Pack Area The Link Pack area (LPA) is the component of MVS that maintains core operating system functions resident in main storage. A security concern exists when libraries from which LPA modules are obtained require APF authorization.			
32.	Do the LPA libraries only contain required modules to support the system?	The LPA libraries should only contain required modules to support the system?		

Step #	Procedure Description SYSTEM INTEGRITY	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
	Linklist The Linklist is a default set of libraries that MVS will search for a specified program. This facility is used so that a user does not have to know the library names in which utility types of programs are stored. Control over membership in the Linklist is specified within the operating system.			
33.	Is the parameter LINKAUTH=APFTAB define to the parmlib?	This requires that all libraries in the Linklist needing APF authorization be specified in a member of the parmlib, and that the linklist is not automatically authorized which is the IBM default.		
	SMF Data Collection SMF data presents a critical component in providing the required audit trails to maintain system integrity. Options for SMF data recording are controlled by the parameters of SYS1.PARMLIB(SMFxxxx).			
34.	Are SMF parameters activated on the system?	SMF parameters should be activated on the system. Some of the SMF parameters critical to the collection process are: **Active** – Activates SMF data collection **JWT(XX)** – Maximum amount of consecutive time that an executing job may spend as ineligible to use any CPU resources before being canceled for inactivity. **MAXDORM(XXXX)** – Specifies the amount of real-time that SMF allows data to remain in an SMF buffer before it is written to a recording data set. **SID** – Specifies the system ID to be recorded in all SMF records. **SYS(DETAIL)** – Controls the level of detail recorded. **SYS(INTERVAL)** – Ensures the periodic recording of data for long-running jobs. **SYS** - Specifies the types and sub-types of SMF records that will be collected. **SYS(TYPE)** indicates that the supplied list is inclusive (i.e., specifies the record types to be collected). Record types not listed are not collected. **SYS(NOTYPE)** indicates that the supplied list is exclusive (i.e., specifies those record types not to be collected). Record types not listed will be collected. The site may use either form of this parameter to specify SMF record type collection		
35.	Is there a mechanism in place to monitor SMF records?	There should be a mechanism in place to monitor SMF records.		

Step #	Procedure Description SYSTEM INTEGRITY	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
36.	Is SMF data collected in a timely manner?	SMF data should be collected in a timely manner.		
37.	Are SMF data sets properly secured and restricted to only authorized personnel?	SMF data should be properly secured and only authorized personnel should have access to the resource.		
	SYSTEM DATA SET and RESOURCE INTEGRITY			
38.	Are system data sets and resources protected on the system, routinely audited, and restricted to only authorized personnel?	Critical system data sets and resources should be protected on the system. The access to the system data sets should be to only authorized personnel and any change / modify to the system data sets should be routinely audited and logged on the system. The default access to these resources should be set to none.		
	System Catalogs (Master Catalog and User Catalogs)			
	System Libraries (LinkList, LPA, SVC, parmlib, IODF (Input/Output Definition File, NUCLEUS))			
	System-Level product libraries (CA-1)			
	Security Software files and databases			
	JES2 SPOOL file (SYS1.HASPACE)			
	JES2 SPOOL checkpoint file (SYS1.HASPCKPT)			
	User attribute data set (SYS1.UADS)			
	SMF data files (SYS1.MANx)			
	System and subsystem trace data sets (e.g., GTF, OS/390 Component Trace)			
	System dump data sets (SYS1.DUMPXX)			
	Logs (JES, SDSF, CICS)			
	Backups, dumps, and off-loads of the above resources (JES2 SPOOL off-loads, external writer output from SYSLOG, SMF dumps, system DASD dumps)			
	System page data sets (PLPA, COMMON, and Local)			
	FACILITY, OPERCMDS resources			
	SYSTEM AND FILE LOCATION File location is an often-overlooked factor in system integrity.			
39.	Are the primary and alternate security databases in separate physical locations or separate volumes?	Avoid collocation of files such as primary and alternate security databases. (i.e. separate physical locations or volumes)		
40.	Are system resources and sensitive data set files reasonably segregated from each other on separate physical volumes?	It is important to ensure that the effects of hardware failures on system integrity and availability are minimized.		

Step #	Procedure Description SYSTEM INTEGRITY	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
	SYSTEM AND FILE BACKUP Adequate backup scheduling is also an often-overlooked integrity exposure. Back up system backup files on a regular schedule.			
41.	Are system and file backups stored at an off-site location?	Backups should be stored off-site to prevent concurrent loss of the live production system and the backup files.		
42.	Are system and file backup routines schedule to process at different times?	Backup scheduling should vary depending on the requirements and capabilities of the individual data center.		
43.	Are system and file backups tested and validated for restorability?	System and file backups should be tested and validated to ensure that the system and files can be restored.		
	SYSTEM AND FILE RECOVERY System and file recovery procedures are essential to the environment			
44.	Does the data center have backup and recovery procedures in place in the event of a disaster or system outage?	There should be written procedures regarding data center backup and recovery activities in the event of a disaster or system outage.		
45.	Have the system backup and recovery procedures been validated and tested by the appropriate personnel?	System backup and recovery procedures should be validated and tested by the appropriate personnel.		

Comments:
Action Plan:

Test Number: **2**	SITE:	DATE:	TIME:
Test Name: **OS/390 UNIX SYSTEM SERVICES**			
Resources Required:	Mainframe Terminal Access		
Personnel Required:	Systems Programmer/Systems Administrator		
Objectives:	Provide high-level overview of the OS/390 UNIX System Services that are associated to the mainframe and have security implications to the environment. For further details regarding this section, please refer to the OS/390 UNIX documentation.		
Procedure Description: (Summary)	Verify that the OS/390 UNIX System has been configured to meet USDA requirements.		

Detailed Procedures and Results

Step #	Procedure Description OS/390 UNIX SYSTEM SERVICES	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
	SECURITY CONTROLS			
	SYS1.PARMLIB Requirements			
1.	Is the BPXPRMxx established with the correct parameters in order to configure OS/390 UNIX properly?	The BPXPRMxx should be established with the correct parameters in order to configure OS/390 UNIX properly. Security Impacting Parameters are: SUPERUSER, TTYGROUP, STELIBLIST, ROOT, MOUNT, USERIDALIASTABLE, FILESYSTYPE, RUNOPTS STARTUP_PROC,		
2.	Are the CSVRTLxx, IEASYSxx, IEFSSNxx, and SMFPRMxx PARMLIB members reviewed for the security impacts for OS/390 UNIX?	The CSVRTLxx, IEASYSxx, IEFSSNxx, and SMFPRMxx PARMLIB members should be reviewed for the security impacts for OS/390 UNIX.		
	/etc Requirements			
3.	Are the /etc directories established and reviewed for the proper configurations in order to reduce the security impacts to the system?	The following /etc directories should be established and reviewed for the proper configurations in order to reduce the security impacts to the system. /etc/auto.master & /etc/mapname /etc/inetd.cof /etc/profile /etc/rc /etc/steplib /etc/tablename		

Step #	Procedure Description OS/390 UNIX SYSTEM SERVICES	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
	Resource Profiles			
4.	Are the OS/390 UNIX resources established properly within the security software?	The OS/390 UNIX resources should be established properly within the security software. FACILITY Class BPX Resources FACILITY Class Resources for RTLS SURROGAT Class BPX Resources FACILITY Class Resources for CA SAF HFS (ACF2, TOP SECRET) FACILITY class Resources for Default User Values in (RACF) UNIXPRIV Class Resources UNIXMAP Class Resources (RACF)		
	OS/390 UNIX MVS Data Sets			
5.	Are security rules defined to prevent unauthorized access changes to the OS/390 UNIX components that have a security impact to the system?	Security rules should be defined to prevent unauthorized access changes to the OS/390 UNIX components that have a security impact to the system. SYS1.ABPX* SYS1.AFOM* SYS1.BPA.ABPA* SYS1.CMX.ACMX* SYS1.SBPX* SYS1.SFOM* SYS1.CMX.SCMX* SYS1.OE.ROOT SYS3.OE.ETCFILES		
	Data Storage – Hierarchical File System (HFS) Directories and Files The file hierarchy is made up of a collection of HFS data sets. Each physical HFS data set is actually a mountable file system. HFS data sets can contain the root file system.			
6.	Are the HFS file systems that contain the root file system defined and restricted on the mainframe?	The HFS file systems that are defined on the mainframe and contain the root file system should have restricted access authorization.		
7.	When deleting UIDs from the system are all associated files removed or deleted from the UID?	UIDs that are deleted from the system should have all associated resources deleted. This prevents object reuse of user resources.		
8.	Are audit attributes for files or directories utilized on the system?	Activities on the HFS file system should be logged on the system.		

Step #	Procedure Description OS/390 UNIX SYSTEM SERVICES	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
	User Identity – UID, GID, and Extended Services IDs defined to the security software and utilize the OS/390 UNIX services are assigned values. IDs are associated with a UID and groups are associated with a GID.			
9.	Are UIDs and GIDs uniquely defined to the system within the security software?	The UIDs and GIDs should be uniquely defined on the system within the security software.		
10.	UIDs with a value of zero have the ability to bypass all security checks. Are UID values reviewed to ensure they are not established with a value of zero?	UIDs should not be established with a value of zero which is equivalent to root authority.		
11.	Are UIDs (such as BPX Super User) with a value of zero audited routinely?	UIDs (such as BPX Super User) with a value of zero should be routinely audited.		
12.	Are the special processing IDs for the OS/390 UNIX established with the appropriate privileges and granted access to the necessary system resources?	The special processing IDs for the OS/390 UNIX should be established with the appropriate privileges and granted access to the necessary system resources. Examples: MVS started tasks UNIX daemons UNIX servers OMVSKERN/OMVS BPXROOT RMFGAT SAS Security Transport		
13.	Are groups defined for special processing IDs for the OS/390 UNIX defined with a GID number between 1-99 or a set of unique range of GID numbers?	Groups defined for special processing IDs for the OS/390 UNIX should be defined with a GID number between 1-99 a set of unique range of GID numbers.		
14.	Are daemons or servers assigned an ID in the security software?	Daemons or servers should be assigned an ID in the security software.		
15.	Are daemons assigned an ID and established with a UID of 0?	Daemons should be assigned an ID and established with a UID of 0. Examples: Cron, Syslogd ,inetd		
16.	Are the appropriate security resources in place to support OS/390 UNIX Background Processes?	The appropriate security resources should be in place to support OS/390 UNIX Background Processes. Examples: BPX.Daemon, BPX.Server		

Step #	Procedure Description OS/390 UNIX SYSTEM SERVICES	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
17.	Is the security software's program control feature active?	The security software's program control feature should be active. All programs should be loaded into the address space and defined to Program Control. Programs in the HFS files should have the program-controlled extended attribute bit set.		
	Interactive Environment – The UNIX Shell Certain commands available to users can have security implications due to their impact on altering security attributes for a directory or file, and impact to systems operations and user privileges. This component provides an interactive UNIX environment to the OS/390 users. The OS/390 UNIX Shell allows users to invoke shell commands or utilities, write shell scripts using the shell programming language, and run shell scripts and C-language programs in foreground, background or batch.			
18.	Are Commands with Security Impacts to the environment properly defined and secured on the system?	Commands with Security Impacts to the environment should be secured on the system. Examples: **Operator Commands:** F BPXOINIT, TERM=pid.tid F BPXOINIT,FORCE=pid.tid F BPXOINIT,SHUTDOWN=FORKINIT F BPXOINIT,SHUTDOWN=FORKS FBPXOINIT,RESTART=FORKS SET OMVS=xx SETOMVS xxx=yy **Sensitive User Commands TSO/E Environment:** ishell Mount, unmount **Sensitive User Commands UNIX Shell Environment:** at, automount, batch chaudit, chgrp, chmod, chown, chroot, crontab, extattr, su		

Step #	Procedure Description OS/390 UNIX SYSTEM SERVICES	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
19.	Are sensitive support variables to control the environment for each user established properly?	Sensitive support variables to control the environment for each user should be established properly. Examples: HOME LOGNAME SHELL PATH STEPLIB _ *BPX* _ACCT_DATA _*BPX* _JOBNAME _*BPX* _USERID		
	SMF			
20.	Are the proper resources established to record SMF data for the OS/390 UNIX processes?	The proper resources should be established to record SMF data for the OS/390 UNIX processes. **Type 30** – User Identity, program name, file system activity. **Type 92** – I/O activity of user or application against a specific file [subtypes 10,11 can be suppressed due to high volume activity]. *Note: Reference SMFPRM member.*		
	Account Data Validation IEFUJI IEFUJI is an OS/390 exit that can be used to validate job names and/or accounting information.			
21.	Is the OMVS defined as a subsystem in the system parmlib (IEFSSNXX)?	The OMVS should be defined as a subsystem in the system parmlib (IEFSSNXX).		
22.	Is IEFUJI setup as an exit for the subsystem OMVS in the system parmlib (SMFPRMXX)?	IEFUJI should be setup as an exit for the subsystem OMVS in the system parmlib (SMFPRMXX).		
23.	Is the IEFUJI code change/ modify to exclude the names of some jobs and daemons started from /etc/rc?	The IEFUJI code should be change/ modify to exclude the names of some jobs and daemons started from /etc/rc.		
	Run-Time Library Services (RTLS) used for OS/390 UNIX			
24.	Is the RUNOPTS parameter coded in the system parmlib (BPXPRMXX)?	The RUNOPTS parameter should be coded in the system parmlib (BPXPRMXX).		
25.	Is the RTLS feature configured in the system parmlib (CSVRTLXX)?	The RTLS feature should be configured in the system parmlib (CSVRTLXX).		

Step #	Procedure Description OS/390 UNIX SYSTEM SERVICES	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
26.	Are the following resources defined in the security software: CSVRTLS.LIBRARY.library.version OR CSVRTLS.NOSECCONNECT.library.version OR CSVRTLS.NOSECCONNECT.*	The following resources should be defined to the security software: CSVRTLS.LIBRARY.library.version For each logical RTLS library to enable security OR CSVRTLS.NOSECCONNECT.library.version For each logical RTLS library to disable checking OR CSVRTLS.NOSECCONNECT.* To disable all RTLS security checking.		

Comments:
Action Plan:

Test Number: **3**	SITE:	DATE:	TIME:
Test Name: **ACF2 RESOURCE CONTROLS**			
Resources Required:	Mainframe Terminal Access		
Personnel Required:	System Programmer / Security Administrator		
Objectives:	Review of ACF2 resource controls		
Procedure Description: (Summary)	Verify that the ACF2 resource controls are configured to meet USDA policies and requirements.		

Detailed Procedures and Results

Step #	Procedure Description ACF2 RESOURCE CONTROLS	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
	GLOBAL OPTIONS **Parameter and Description**	**DEFAULT SETTINGS**		
1.	**APPLDEF** Defines the format of site-defined and other structured Infostorage application records.	Site defined. *NOTE: Local changes should be justified in writing with supporting documentation.*		
2.	**AUTHEXIT** Contains the vendor or site exit information that supports an extended authentication facility, such as operator identification (OID) card support.	AUTHEXIT.001 LIDFIELD(AUTHSUP1) PROCPGM(AUTHXNCP) NOINFOSTG		
3.	**AUTOERAS** Controls the automatic physical erasure of VSAM or non-VSAM data sets.	Unclassified Systems: NONON-VSAM NOVSAM VOLS() Classified Systems: NON-VSAM VSAM VOLS(-) *CAUTION: Will affect performance.*		
4.	**BACKUP** Provides the ability to dynamically maintain the space allocation and location of the ACF2 sequential backup work files. This record also contains the CPU, command string information, and time when the automatic database backup utility is to occur.	Site defined.		

Step #	Procedure Description ACF2 RESOURCE CONTROLS	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
5.	**BLPPGM** Specifies those programs authorized to use tape bypass label processing (BLP.	None should be specified. *NOTE: BLP enforcement should be done based on **LID record settings**.*		
6.	**CLASMAP** (Version 6.0 and above) Translates an eight-character SAF resource class into a three-character ACF2 resource type code to enable resource rules to be written to perform validation. Also it translates the resource type codes for ACF2 calls or calls made to ACF2 from CA's International Standard Security Facility (CAISSF).	Site defined. *NOTE: Local changes should be justified in writing with supporting documentation.* *Ensure that CONSOLE is defined as TYPE(CON), FACILITY is defined as TYPE(FAC), OPERCMDS is defined as TYPE(OPR), and TSOAUTH is defined as TYPE(TSO*		
7.	**EXITS** Specifies the module names of site-written ACF2 exit routines.	DSNPOST(module) SEVPRE(SEVPRE01) SEVPOST(SEVPST01) *NOTE: Local changes should be justified in writing with supporting documentation.*		
8.	**INFODIR** Specifies the Infostorage directories and rule sets that are to be made resident at ACF2 initialization time. *NOTE: CA recommends that INFODIR records be used, rather than RESDIR records.*	Site defined. All resource types applicable for masking will be specified as resident.		
9.	**LINKLST** Specifies one or more partitioned data sets considered part of the system link (**SYS1.LINKLIB**) during data set access validation.	Site defined. Only trusted system data sets should be listed, **not** all libraries in the system Linklist. Application libraries will never be included.		
10.	**LOGPGM** Specifies those programs for which all accesses for all data sets are logged	Site defined.		
11.	**MAINT** Specifies the logonid, program, and library combinations used for system maintenance functions. *NOTE: For logonIDs that match environments described in records, **no** SMF logging records should be created.*	Site defined. *NOTE: Local changes should be justified in writing with supporting documentation.*		

Step #	Procedure Description ACF2 RESOURCE CONTROLS	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
12.	**NJE** Specifies ACF2 validation options that apply to jobs submitted through a network job entry subsystem (JES2 JES3 RSCS).	DFTLID() INHERIT NODEMASK(-) ENCRYPT VALIN(YES) NOVALOUT *NOTE: For NJE nodes that are incompatible with the XDES algorithm, discrete NJE records should be created with NOENCRYPT.* *NOTE: Local changes should be justified in writing with supporting documentation.*		
13.	**OPTS** Defines the global options available to the system.	BLPLOG NOCACHE NOCMDREC CONSOLE(NOROLL) CPUTIME(LOCAL) DATE(MDY) NODDB DFTLID() DFTSTC() INFOLIST(SECURITY, AUDIT) JOBCHK MAXVIO(10) MODE(ABORT) NOTIFY RPTSCOPE SAF (pre-6.0 only) SHRDASD STAMPSMF STC TAPEDSN NOUADS NOXBM NOVTAMOPEN		
14.	**PPGM** Defines protected programs that can only be executed by privileged users.	PGM-MASK(pgm-mask1, ...,pgm-mask255)		
15.	**PSWD** Defines various logonid password options and controls.	MAXTRY(3) MINPSWD(6) PASSLMT(5) PSWDALT PSWDFRC PSWDJES NOPSWDXTR WRNDAYS(10)		

Step #	Procedure Description ACF2 RESOURCE CONTROLS	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
16.	**RESDIR** Specifies resource rule directories that are to be made globally resident at ACF2 initialization time. *NOTE: CA recommends that INFODIR records be used, rather than RESDIR records. RESDIR records should be migrated to INFODIR records at the earliest convenience of the sites.*	Site defined. All resource types applicable for masking should be specified as resident.		
17.	**RESRULE** Specifies data set access rules that are to be made resident at ACF2 initialization time.	None. *NOTE: Local changes should be justified in writing with supporting documentation.*		
18.	**RESVOL** Defines the DASD and mass storage volumes for which ACF2 is to provide data set-level protection.	VOLMASK(-) *NOTE: Local changes should be justified in writing with supporting documentation.*		
19.	**RULEOPTS** Specifies the options pertinent to access and resource rule maintenance and where resident rules and resident resource rule directories are built into an MVS or MVS/ESA environment.	ACCRULE(ANY) CENTRAL CHANGE DECOMP(SECURITY,AUDIT) NO$NOSORT NOPATHTRAN RSCDIR(ANY) RSCRULE(ANY) NOVOLRULE		
20.	**SAFDEF** (Version 6.0 and above) Defines System Authorization Facility (SAF calls that each site may want to process differently than the default ACF2 process.	No change from defaults. *NOTE: Local changes should be justified in writing with supporting documentation.*		
21.	**SECVOLS** Defines those DASD mass storage, and tape volumes for which ACF2 is to provide volume-level protection.	None. *NOTE: Local changes should be justified in writing with supporting documentation.*		
22.	**SYNCOPTS** Defines the cache synchronization processing for a CPU running in a shared ACF2 database environment.	FILENAME(ACF2.SYNCFILE) POLLINTV(10) USECOUNT(10) NOACTIVATE		

Step #	Procedure Description ACF2 RESOURCE CONTROLS	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
23.	**TSO** Specifies global usage and system parameters that define and control the TSO logon process and other system parameters.	ACCOUNT(1) BYPASS(#) CHAR(BS) CMDLIST() NOFSRETAIN LINE(ATTN) LOGONCK PERFORM(0) PROC(IKJACCNT) NOQLOGON REGION(site defined) SUBCLSS() SUBHOLD() SUBMSG() TIME(0) TSOSOUT(A) UNIT(SYSDA) WAITIME(60) or less		
24.	**TSOCRT** Defines a clear string used to obliterate the logon to ASCII CRT devices.	STRING(A12FA11C1A270C0D)		
25.	**TSOKEYS** Defines site-supplied keywords permitted by ACF2at TSO logon time.	KEYWORDS()		
26.	**TSOTWX** Defines a cross-out mask to obliterate the logon password on TWX devices.	CR(15) IDLE(17) LENGTH(8) M1(X) M2(N) M3(Z) M4(M) STRING()		
27.	**TSO2741** Defines a cross-out string used to obliterate the logon password on 2741 devices.	BS(16) LENGTH(8) M1(X) M2(N) M3(Z) M4(M) STRING()		
28.	**WARN** Specifies text of a warning message to be displayed on the terminal and job log when a violation takes place and the ACF2 system is in WARN mode.	Warning Message should be display. However, systems should be in fail mode.		
	USER Profile Settings **A sample of user ids should be verified.**			
29.	Is every user defined to the system identified with a unique logonid?	All users defined to the system should be defined with a unique logonid.		
30.	Are all fields comprised of the UID-string filled out for each user's logonid?	The UID-string should be filled out for every logonid to properly identify users to the system.		

Step #	Procedure Description ACF2 RESOURCE CONTROLS	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
	User Profile **Parameter and Description**	**DEFAULT SETTINGS**		
31.	**ALLCMDS/NOALLCMDS** Ability to bypass ACF2 restricted command lists.	NOALLCMDS		
32.	**AUTHSUP1** User Authorization Flag 1	ON for highly privileged users controlled by NC-PASS.		
33.	**CONSOLE/NOCONSOLE** Permits access to the TSO/E CONSOLE facility.	NOCONSOLE The CONSOLE bit will not be turned on unless command-level controls are implemented.		
34.	**GROUP(name)** This field is required for assigning *gIDs* to MVS OpenEdition users. *NOTE: For sites running UNIX Systems Services.*	Should be defined for OpenEdition users.		
35.	**IDLE(time)** Specifies the maximum time permitted (in minutes) between terminal transactions for this user. If exceeded, ACF2 needs the logonid and password to be revalidated before another transaction is accepted. Zero (0) indicates no limit is enforced. This field is available for IMS and CICS on-line processing.	IDLE(15)		
36.	**INTERCOM/NOINTERCOM** Indicates this user is willing to accept messages from other users through the TSOSEND command.	INTERCOM		
37.	**LGN-ACCT/ NOLGN-ACCT** Indicates permission to specify an account number at logon time. If a user has the PMT-ACCT field, ACF2 prompts the user for an account number unless an account number is specified before the prompt. If a user does not specify an account number at logon and PMT-ACCT is not specified in the user's logonid record, ACF2 uses the user's default account number (TSOACCT is the logonid field) or the system default account number. Specifies the default in the ACCOUNT field of the GSO TSO record.	LGN-ACCT		
38.	**MAIL/NOMAIL** Indicates a user can receive mail messages from TSO at logon time.	MAIL		

Step #	Procedure Description ACF2 RESOURCE CONTROLS	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
39.	**MAXDAYS(days)** Specifies the maximum number of days permitted between password changes before the password expires. Zero (0) indicates no limit.	MAXDAYS (90)		
40.	**MINDAYS(days)** Specifies the minimum number of days that must elapse before a user can change a password Zero (0) indicates no limit.	MINDAYS (1)		
41.	**MOUNT/NOMOUNT** Permission to issue mounts for devices.	NOMOUNT		
42.	**MSGID/NOMSGID** Indicates this user wants TSO messages to have message IDs prefixed.	MSGID		
43.	**NAME(username)** Specifies the 1- to 20-character name of the user. ACF2 displays this name on logging and security violation reports. ACF2 also uses this name as the NAME field of the job statement created for a TSO logon session, if the NOUADS field is specified in the GSO OPTS record.	Name field should be completed for all users.		
44.	**NON-CNCL/NONON-CNCL** ACF2 cannot cancel the user for security violations. Access is permitted but logged.	NONON-CNCL		
45.	**NO-STORE/NONO-STORE** Specifies that a user cannot store or delete rule sets. This applies even if the value of the PREFIX field of the logonid record matches the $KEY of the rule of the data set, if the user has the SECURITY privilege, or if the user has change authority through a %CHANGE or %RCHANGE control statement in the rule set.	NONO-STORE		
46.	**NOTICES/NONOTICES** Indicates a user can receive TSO notices at logon time.	NOTICES		
47.	**OPERATOR/NOOPERATOR** User has TSO operator privileges.	NOOPERATOR		
48.	**PASSWORD** The logon password for the user.	Field should be completed.		
49.	**PHONE** Specifies the 1- to 12-character telephone number of a user.	Optional		

Step #	Procedure Description ACF2 RESOURCE CONTROLS	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
50.	**PMT-ACCT/NOPMT-ACCT** Indicates that ACF2 requires a user to specify an account at logon time and to specify the LGN-ACCT field also. ACF2 does not prompt for an account number if the FSRETAIN field is also specified. FSRETAIN obtains account values from the last session.	PMT-ACCT		
51.	**PPGM/NOPPGM** User can execute protected programs specified in the GSO PPGM record.	NOPPGM		
52.	**PREFIX** User access to the user's own data sets without rule validation.	PREFIX()		
53.	**PROMPT/NOPROMPT** Indicates that ACF2 prompts a user for missing or incorrect parameters.	PROMPT		
54.	**RESVLD/NORESVLD** Indicates that an access rule must validate any resource accesses that the user makes. Applies even if the user has ownership of the resource, or has the SECURITY attribute.	RESVLD		
55.	**RULEVLD/NORULEVLD** Indicates that an access rule must validate any data set accesses that the user makes. Applies even if the user has ownership of the data set, or has the SECURITY attribute.	RULEVLD		
56.	**TSOACCT** Specifies the user's default TSO logon account. Used for all billing.	May be required for support.		
57.	**TSOPROC** Specifies the user's default TSO logon procedure.	Field should be completed for all TSO users.		
58.	**TSOPROC** Specifies the user's default TSO logon procedure.	Field should be completed for all TSO users.		
59.	**UID-String Fields** All fields defined in the @UID macro in the ACFFDR. UID-string fields currently are locally defined on each system. Their composition and contents should be fully documented.	Field should be completed. *NOTE: Only those fields necessary to restrict the user to those accesses and functions required to perform assigned tasks are required.*		

Step #	Procedure Description ACF2 RESOURCE CONTROLS	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
60.	**VLD-ACCT/NOVLD-ACCT** Indicates that ACF2 validates the TSO account number of a user. Creates a resource rule with a type code TAC and a $KEY of the account number so that ACF2 will perform this validation.	VLD-ACCT May be required for support.		
61.	**VLD-PROC/NOVLD-PROC** Indicates that ACF2 validates the TSO logon procedure of a user. Creates a resource rule with a type code TPR and a $KEY of the logon procedure so that ACF2 will perform this validation.	VLD-PROC Field should be completed for all TSO users.		
	SPECIAL PROCESSING IDS for Business Applications, Administration, and system support functions			
	Batch Processing IDs			
62.	Are Batch Processing IDs established as default IDs on the system?	Batch Processing IDs should not be established as default IDs on the system.		
63.	Are Batch Processing IDs established with only minimum authority on the system necessary to perform its function?	Batch Processing IDs should only be established with minimum authority on the system necessary to perform its function.		
64.	Are Batch Processing IDs distinguished from the general TSO user IDs on the system?	Batch Processing IDs should be distinguished from the general TSO user IDs on the system.		
65.	Are submissions for Batch Processing IDs using a job scheduler?	Batch submissions should be using a job scheduler.		
66.	Are the following parameters set for Batch Processing IDs: RESTRICT PGM(XXXXXXX) and SUBAUTH SOURCE (XXXXXXXX)	Batch Processing IDs should be defined with the following parameters: RESTRICT PGM(XXXXXXX) and SUBAUTH SOURCE (XXXXXXXX)		
	Started Task Control IDs			
67.	Are Started Task IDs established as default IDs on the system?	Started Task IDs should not be established as default IDs on the system.		
68.	Are Started Task IDs established with only minimum authority on the system necessary to perform its function?	Started Task IDs should only be established with minimum authority on the system necessary to perform its function.		
69.	Are Started Task IDs distinguished from the general TSO user IDs on the system?	Started Task IDs should be distinguished from the general TSO user IDs on the system.		

Step #	Procedure Description ACF2 RESOURCE CONTROLS	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
70.	Are the following parameters set for Started Task IDs: STC MUSASS & NO-SMC – if the Started Task is for MUSASS JOBFROM – If there is requirement to submit jobs on behalf of users MUSUPDT – If there is a requirement to update information in the ACF2 database	Started Task IDs should be defined with the following parameters: STC MUSASS & NO-SMC – if the Started Task is for MUSASS JOBFROM – If there is requirement to submit jobs on behalf of users MUSUPDT – If there is a requirement to update information in the ACF2 database		
	Storage Management IDs			
71.	Are Storage Management IDs established as default/generic IDs on the system with only minimum authority on the system necessary to perform its function?	Storage Management IDs should not be established as default/generic IDs on the system and should only be established with minimum authority on the system necessary to perform its function.		
72.	Are Storage Management IDs established as default/generic IDs on the system?	Storage Management IDs should only be established with minimum authority on the system necessary to perform its function.		
73.	Are Storage Management IDs distinguished from the general TSO user IDs on the system?	Storage Management IDs should be distinguished from the general TSO user IDs on the system.		
74.	Are the following parameters set for Storage Management IDs: JOB MAINT	Storage Management IDs should be defined with the following parameters: JOB MAINT		
	Emergency IDs			
75.	Are there separate emergency IDs to perform operating and administrative functions on the system?	There should be separate emergency IDs to perform operating and administrative functions on the system.		
76.	Are the activities from the emergency IDs logged on the system?	All activities from the emergency IDs should be logged on the system.		
77.	Are there documented procedures for the use and release of the emergency IDs?	There should be documented procedures for the use and release of emergency IDs.		
78.	Are the following parameters set for Emergency IDs:	Emergency IDs should be defined with the following parameters:		

Step #	Procedure Description ACF2 RESOURCE CONTROLS	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
	Only ability to access/update data sets: NOFSRETAIN JCL JOB MONITOR NON-CNCL PMT-ACCT TSO TSOPROC(xxxxxxxx) TSOACT(none)	Only ability to access/update data sets: NOFSRETAIN JCL JOB MONITOR NON-CNCL PMT-ACCT TSO TSOPROC(xxxxxxxx) TSOACT(none)		
	Only security administration privileges with no access to update system data sets: ACCOUNT NOFSRETAIN JCL JOB MONITOR NONON-CNCL RULEVLD SECURITY PMT-ACCT TSO TSOPROC(xxxxxxxx) TSOACCT(none)	Only security administration privileges with no access to update system data sets: ACCOUNT NOFSRETAIN JCL JOB MONITOR NONON-CNCL RULEVLD SECURITY PMT-ACCT TSO TSOPROC(xxxxxxxx) TSOACCT(none)		
	REFRESH IDs			
79.	Are the refresh IDs activated and deactivated only when required for system use?	Refresh IDs should only be activated when needed and deactivated when not in use.		
80.	Are the following parameters set for REFRESH IDs: REFRESH SUSPEND	REFRESH IDs should be defined with the following parameters: REFRESH SUSPEND		
	FTP IDs			
81.	Is Anonymous FTP disabled on the system?	Anonymous FTP should be disabled on the system.		
82.	Are all scripts and/or data files located on the remote(s) that contain the MVS FTP ID and/or password secured and limited to only authorized personnel requiring access?	Secure all scripts and/or data files located on the remote system(s) that contain the MVS FTP ID and/or password (e.g., another OS/390 host or a remote UNIX system). Restrict access to these files to those individuals responsible for the application connectivity and who have a legitimate requirement to know the FTP ID and password.		
83.	Are the FTP IDs defined for only one system or application function?	FTP IDS should be defined for only one system or application function to prevent exposures to other systems.		
84.	Are the activities of the FTP IDS logged on the system?	All activities of the FTP IDS should be logged on the system.		

Step #	Procedure Description ACF2 RESOURCE CONTROLS	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
85.	Are FTP IDs established with only minimum authority on the system necessary to perform its function?	FTP IDs should only be established with minimum authority on the system necessary to perform its function.		
86.	Are FTP IDs established without TSO?	FTP IDs should be established without TSO.		
87.	Are FTP IDs established with non-expiring passwords?	FTP IDs should be established with non-expiring passwords. This is with the understanding that the application owner or group accepts the potential risks to the system.		
88.	Are the following parameters set for FTP IDs: MAXDAYS(0) TRACE TSOCMDS(<command table>)	FTP IDs should be defined with the following parameters: MAXDAYS(0) TRACE TSOCMDS(<command table>)		
	MCS (Multiple Console Support) Console IDs MCS consoles allow operators to enter MVS and JES system commands.			
89.	Are MCS Console IDs defined without TSO or other online privileges?	MCS Console IDs should not be defined with TSO or other segments not required for the operation console.		
90.	Is the only resource MCS Console IDs permitted to access MVS.MCSOPER.consolename?	MCS Console IDs should not be permitted access to any resources except MVS.MCSOPER.consolename.		
91.	If autolog is allowed on the system, is read access permitted for the following commands: CONTROL DISPLAY MONITOR STOPMN STOPTR TRACK	If autolog is allowed on the system then read access should be permitted for the following commands: CONTROL DISPLAY MONITOR STOPMN STOPTR TRACK		
	OS/390 System Operator IDs			
92.	Does each system operator have their own personal system operator ID?	Each system operator should have their own personal system operator ID.		
93.	Where several operators require the same authority to the system, define a sub-string of the UID string that can be used in rule sets instead of specifying the individual operator IDs?	Where there are a group of individuals requiring access to the same resource a sub-string of a UID should be defined to the rule sets instead of the individual operator IDs.		
94.	Are accesses to these resources logged by the system?	Accesses to these resources should be logged by the system.		
	SPECIAL PRIVILEGES			
	Modification Privileges			

Step #	Procedure Description ACF2 RESOURCE CONTROLS	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
	System and Administrator Privileges	Examples: ACCOUNT LEADER SECURITY ACCTPRIV REFRESH AUDIT CONSULT		
95.	Is authority to privileged access on the system limited to authorized personnel?	Authority to privileged access on the system should be limited to only authorized personnel.		
96.	Is authority to privileged access on the system logged and reviewed/monitored routinely?	Authority to privileged access on the system should be logged and reviewed/monitored routinely.		
	Tape Label Bypass Privileges			
97.	Is access to Tape Label Bypass privileges restricted to authorized personnel?	Tape Label Bypass privileges should be restricted to only authorized personnel. Two privileges granted for BLP processing in ACF2: TAPE-LBL TAPE-BLP		
98.	Is the Tape Label Bypass privilege controlled at the user level and not by the tape management system?	Tape Label Bypass privileges should be controlled at the user level and not by the tape management system.		
	Other Sensitive Privileges			
99.	Are Device Mount privileges restricted to authorized personnel?	Device Mount privileges should be restricted to authorized personnel.		
100.	Is access to the TSO/E Console strictly controlled?	Access to the TSO/E Console should be granted on an as-needed basis.		
101.	Are sensitive commands that a TSO user can issue restricted?	TSO users should be restricted from issuing sensitive commands.		

Step #	Procedure Description ACF2 RESOURCE CONTROLS	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
102.	Is the ability to execute privileged programs restricted on the system?	The ability to execute privileged programs should be restricted on the system. Privileged Programs such as: ***GTF** System Activity Trace ***IOCP System Configuration *MASPZAP Data Management ADRDSSU DASD Management AMAZAP Data Management BLSROPTR Data Management DEBE Data Management DITTO Data Management FDRZAPOP Product Internal ICKDSF DASD Management IDCSC01 IDCAMS Set Cache IEHATLAS Data Management IEHD**** DASD Management IEHINITT Tape Management IFASMFDP SMF Data Dump IGWSPZAP Data Management IND$FILE PC to Mainframe *****SCP System Configuration		
103.	Is the ability to access data sets regardless of rule set specifications restricted to only authorized users?	The ability to access data sets regardless of rule set specifications should be restricted to only authorized users.		
104.	Are operator command privileges restricted to authorized personnel?	Operator command privileges should be restricted to only authorized personnel.		
	DATA SET CONTROLS			
105.	Are all data set rules appropriately protected?	All data set rules should be appropriately protected.		
106.	Is global access to data sets used on data set rules restricted at the appropriate level of access?	Global access on data sets should be restricted to the appropriate level of access for general purpose libraries.		
	VOLUME CONTROLS			
107.	If volume-level protection utilized on the system, is it controlled using SECVOLS and RESVOLS records?	When volume-level protection is required it should be controlled using SECVOLS and RESVOLS records.		
	SENSITIVE UTILITY CONTROLS Utilities are essential to data center operations and support. Tape Management, DASD Management, Job Scheduling, Storage Alteration, System Modification			
108.	Is access to sensitive utilities appropriately defined?	Access to sensitive utilities should be appropriately defined.		
109.	Are the resources relating to sensitive utilities appropriately controlled and defined?	Access to the resources relating to sensitive utilities should be appropriately controlled and defined.		
110.	Are accesses to the resource audited by the system?	Accesses to the resource should be audited by the system.		

Step #	Procedure Description ACF2 RESOURCE CONTROLS	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
111.	Is execution access to sensitive utilities controlled through the use of the facilities: MAINT, PPGM, LOGPGM?	Execution access to sensitive utilities should be controlled through the use of the facilities: MAINT, PPGM, LOGPGM.		
	DYNAMIC LIST CONTROLS Dynamic List Controls are provided via resources in the FACILITY resource class.			
112.	Are generic and specific resource rules defined to prevent access by default?	Generic and specific resource rules should be defined on the system to prevent access by default system settings.		
113.	Are all accesses to the resource logged by the system?	Accesses to the resource should be logged by the system.		
114.	Is access to the resource limited to only authorized personnel?	Access to the resource should be limited to only authorized personnel.		
115.	Are dynamic list controls defined under the FACILITY resource class?	Dynamic List controls should be defined under the FACILITY resource class.		
	CONSOLE CONTROLS Consoles are protected via resources in the CONSOLE, FACILITY, OPERCMDS, and TSOAUTH resource classes. Console controls allow an installation to restrict access to operator consoles and allow a secure replacement of various 3rd party console facilities.			
116.	Are only the resource MCS Console IDs permitted to access MVS.MCSOPER.consolename?	MCS Console IDs should not be permitted access to any resources except MVS.MCSOPER.consolename.		
117.	Are all accesses to the resource logged by the system?	Accesses to the resource should be logged by the system.		
	OS/390 SYSTEM COMMAND CONTROLS			
118.	Are OS/390 system command controls defined under the OPERCMDS resource class?	The OS/390 system command controls should be defined under the OPERCMDS resource class.		
119.	Are all accesses to the resource logged by the system?	Accesses to the resource should be logged by the system.		

Comments:
Action Plan:

Test Number: **4**	SITE:	DATE:	TIME:
Test Name: **RACF RESOURCE CONTROLS**			
Resources Required:	Mainframe Terminal Access		
Personnel Required:	Systems Programmer/Security Administrator		
Objectives:	Review of RACF Resource Controls		
Procedure Description: (Summary)	Verify that the RACF resource controls are configured to meet USDA policies and requirements.		

Detailed Procedures and Results

Step #	Procedure Description RACF RESOURCE CONTROLS	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
	GLOBAL OPTIONS **Parameter and Description**	**DEFAULT SETTINGS**		
1.	**ADSP** Automatic data set protection	NOADSP		
2.	**AUDIT** Logging RACF command and RACDEF SVC activity	AUDIT(*)		
3.	**CLASSACT** General resource protection	The following classes should be activated on all systems: DATASET, USER, GROUP The following class should be activated only if no tape management system is installed on the system: TAPEVOL All general resources used by a given system MUST be identified to RACF for protection.		
4.	**CMDVIOL** Logging of RACF command violations	CMDVIOL		
5.	**EGN** Enhanced generic naming	EGN		
6.	**ERASE** Erasure of scratched or released DASD data set space.	Unclassified Systems: ERASE() Classified Systems: ERASE(ALL) *NOTE: Will affect performance. May be implemented in DSN profiles, which would afford more granular control. This use should be documented by the ISSO.*		
7.	**GENCMD**	GENCMD(*)		

Step #	Procedure Description RACF RESOURCE CONTROLS	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
	Generic profile creation			
8.	**GENERIC** Generic profile checking	GENERIC(*)		
9.	**GLOBAL** Global access checking	Site defined		
10.	**GRPLIST** List-of-Groups authority checking	GRPLIST		
11.	**INACTIVE** Unused userid interval	35 days		
12.	**INITSTATS** Records RACINIT statistics	INITSTATS		
13.	**JES(BATCHALLRACF)** Forces batch users to identify themselves to RACF	JES(BATCHALLRACF)		
14.	**JES(EARLYVERIFY)** JES userid early verification	JES(EARLYVERIFY)		
15.	**JES(XBMALLRACF)** Support for execution batch monitor	JES(XBMALLRACF)		
16.	**MODEL** Data set modeling	Site defined.		
17.	**OPERAUDIT** Logging activities of users with the OPERATIONS attribute	OPERAUDIT		
18.	**PASSWORD (HISTORY)** Number of previous passwords	10		
19.	**PASSWORD (INTERVAL)** Maximum password change interval	90 days		
20.	**PASSWORD (REVOKE)** Consecutive password verification attempts	3		
21.	**PASSWORD (RULEnO)** Password syntax rules	MIN=(6) ALPHA-NUMERIC (1 ALPHA, 1 NUMERIC)		
22.	**PASSWORD (WARNING)** When password expiration message is issued	10		
23.	**PROTECTALL** RACF-protect all data sets	PROTECTALL This option forces the default protection of all resources, requiring profiles to be written for all resources and data sets.		
24.	**REALDSN** Places actual data set names in messages and SMF records	REALDSN		
25.	**RETPD** Selects security retention period for tape data sets	99999		
26.	**RVARYPW** Sets the RVARY passwords	Site defined. To be set in accordance with standard password guidelines.		
27.	**SAUDIT**	SAUDIT		

Step #	Procedure Description RACF RESOURCE CONTROLS	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
	Logging of activity of users with SPECIAL attribute			
28.	**SECLEVELAUDIT** Auditing for security levels	NOSECLEVELAUDIT		
29.	**STATISTICS** Activates resource statistics collection	Site defined.		
30.	**TAPEDSN** Activates tape data set protection	Site defined based on the requirements of the resident tape management system and the release level of RACF.		
31.	**TERMINAL** Universal access authority for terminals	READ		
32.	**WHEN(PROGRAM)** Program control	WHEN(PROGRAM)		
	USER Profile Settings **A sample of user ids should be verified.**			
	User Profile Parameter and Description	**DEFAULT SETTINGS**		
33.	**ACCTNUM** Specifies the user's default TSO logon account. Used for all billing.	May be required for support.		
34.	**DATA** Installation data field *NOTE: Field may be used for validation by other products (e.g., Netmaster).*	Optional		
35.	**DFLTGRP** User's default group	Field should be completed for all users.		
36.	**NAME(username)** Specifies the 1- to 20-character name of the use.	Field should be completed for all users.		
37.	**OWNER** User's profile owner	Field should be completed for all users.		
38.	**PASSWORD** Logon password for the user	Field should be completed for all users.		
39.	**PROC** Specifies the user's default TSO logon procedure	Field should be completed for all TSO users.		
40.	**SECLABEL** User's current security label	Optional for Class C2		
41.	**USERDATA** Optional user data	Site defined		
	SPECIAL PROCESSING IDS for Business Applications, Administration, and system support functions			
	Batch Processing IDs			
42.	Are Batch Processing IDs established as generic IDs on the system?	Batch Processing IDs should not be established as generic IDs on the system.		
43.	Are Batch Processing IDs	Batch Processing should only be		

Step #	Procedure Description RACF RESOURCE CONTROLS	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
	established with only minimum authority on the system necessary to perform its function?	established with minimum authority on the system necessary to perform its function.		
44.	Are Batch Processing IDs distinguished from the general TSO user IDs on the system?	Batch Processing IDs should be distinguished from the general TSO user IDs on the system.		
45.	Are submissions for Batch Processing IDs using a job scheduler?	Batch submissions should be using a job scheduler.		
46.	Are Batch Processing IDs defined using the SURROGAT resource?	Batch Processing IDs should be defined using the SURROGAT resource.		
	Started Task Control IDs			
47.	Are Started Task IDs established as generic IDs on the system?	Started Task IDs should not be established as generic IDs on the system.		
48.	Are Started Task IDs established with only minimum authority on the system necessary to perform its function?	Started Task IDs should only be established with minimum authority on the system necessary to perform its function.		
49.	Are Started Task IDs connected to a Started Task group?	Started Task IDs should be connected to a Started Task group.		
50.	Is the Started Task group defined with no data set access on the system?	The Started Task group should not be defined with access to data sets on the system.		
51.	Is there a general resource defined for all Started Task IDs?	A general resource should be defined for all Started Task IDs.		
52.	Are Started Task IDs distinguished from the general TSO user IDs on the system?	Started Task IDs should be distinguished from the general TSO user IDs on the system.		
	Storage Management IDs			
53.	Are Storage Management IDs established as default/generic IDs on the system?	Storage Management IDs should not be established as default/generic IDs on the system.		
54.	Are Storage Management IDs with only minimum authority on the system necessary to perform its function?	Storage Management IDs should only be established with minimum authority on the system necessary to perform its function.		
55.	Are Storage Management IDs distinguished from the general TSO user IDs on the system?	Storage Management IDs should be distinguished from the general TSO user IDs on the system.		
56.	Is the DASDVOL or GDASDVOL resource defined?	The DASDVOL or GDASDVOL resource should be defined		
57.	Is the system privilege OPERATIONS authorized to the Storage Management IDs?	The system privilege OPERATIONS should be authorized to the Storage Management IDs.		
	Emergency IDs			
58.	Are there separate emergency IDs (established with System Special or Operations) to perform operating and administrative functions on the system?	There should be separate emergency IDs (established with System Special or Operations) to perform operating and administrative functions on the system.		

Step #	Procedure Description RACF RESOURCE CONTROLS	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
59.	Are the activities from the emergency IDs logged on the system?	All activities from the emergency IDs should be logged on the system.		
60.	Are there documented procedures for the use and release of the emergency IDs?	There should be documented procedures for the use and release of emergency IDs.		
61.	Is audit enabled on emergency IDs?	Audit should be enabled on emergency IDs.		
	FTP IDs			
62.	Is Anonymous FTP disabled on the system?	Anonymous FTP should be disabled on the system.		
63.	Are all scripts and/or data files located on the remote(s) that contain the MVS FTP ID and/or password secured and limited to only authorized personnel requiring access?	Secure all scripts and/or data files located on the remote system(s) that contain the MVS FTP ID and/or password (e.g., another OS/390 host or a remote UNIX system). Restrict access to these files to those individuals responsible for the application connectivity and who have a legitimate requirement to know the FTP ID and password.		
64.	Are the FTP IDs defined for only their system or business application?	FTP IDS should be defined for only a system or a business application to prevent exposures to other systems.		
65.	Are the activities of the FTP IDS logged on the system?	All activities of the FTP IDS should be logged on the system.		
66.	Are FTP IDs established with only minimum authority on the system necessary to perform its function?	FTP IDs should only be established with minimum authority on the system necessary to perform its function.		
67.	Are FTP IDs for business functions established without TSO?	FTP IDs for business functions should be established without TSO.		
68.	Are FTP IDs established with non-expiring passwords?	FTP IDs should be established with non-expiring passwords. This is with the understanding that the application owner or group accepts the potential risks to the system.		
	MCS (Multiple Console Support)Console IDS MCS consoles allow operators to enter MVS and JES system commands.			
69.	Are MCS Console IDs defined without TSO or other online privileges?	MCS Console IDs should not be define with TSO or other segments not required for the operation console.		
70.	Is only the resource MCS Console IDs permitted to access MVS.MCSOPER.consolename?	MCS Console IDs should not be permitted access to any resources except MVS.MCSOPER.consolename.		
71.	Is a RACF group profile defined for all MCS Console IDs?	A RACF group profile should be defined for all MCS Console IDs.		
72.	If autolog is allowed, is a second RACF group profile	A second RACF group profile should be defined with READ access to the		

Step #	Procedure Description RACF RESOURCE CONTROLS	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
	defined with READ access to the following: CONTROL, DISPLAY, MONITOR, STOPMN, STOPTR, TRACK?	following: CONTROL, DISPLAY, MONITOR, STOPMN, STOPTR, TRACK, if autolog is utilized on the system.		
	OS/390 System Operator IDS			
73.	Does each system operator have their own personal system operator ID?	Each system operator should have their own personal system operator ID.		
74.	Are OS/390 system command controls defined under the OPERCMDS resource class?	The OS/390 system command controls should be defined under the OPERCMDS resource class.		
75.	Are accesses to these resources logged by the system?	Accesses to these resources should be logged by the system.		
	SPECIAL PRIVILEGES			
	Modification Privileges			
	System and Administrator Privileges	Examples: SPECIAL GROUP-SPECIAL OPERATIONS GROUP-OPERATIONS AUDITOR GROUP-AUDITOR		
76.	Is authority to privileged access on the system limited to authorized personnel?	Authority to privileged access on the system should be limited to only authorized personnel.		
77.	Is authority to privileged access on the system logged and reviewed/monitored routinely?	Authority to privileged access on the system should be logged and reviewed/monitored routinely.		
78.	Has separation of duties been maintained in granting SPECIAL, OPERATIONS, and AUDITOR privileges?	Privilege user should not have SPECIAL, OPERATIONS, and/or AUDITOR on a full-time basis.		
	Tape Label Bypass Privileges			
79.	Is access to Tape Label Bypass privileges restricted to authorized personnel?	Tape Label Bypass privileges should be restricted to only authorized personnel.		
80.	Is the Tape Label Bypass privilege controlled at the user level and not by the tape management system?	Tape Label Bypass privileges should be controlled at the user level and not by the tape management system.		
	Other Sensitive Privileges			
81.	Are Device Mount privileges restricted to authorized personnel?	Device Mount privileges should be restricted to authorized personnel.		
82.	Are TSOAUTH privileges for OPER and ACCOUNT restricted to authorized personnel?	TSOAUTH privileges for OPER and ACCOUNT should be restricted to authorized personnel.		
83.	Are sensitive commands that a TSO user can issue restricted?	The sensitive commands that a TSO user can issue should be restricted.		
84.	Is the ability to execute privileged programs restricted	The ability to execute privileged programs should be restricted on the		

Step #	Procedure Description RACF RESOURCE CONTROLS	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
	on the system?	system. Privileged Programs such as: ***GTF** System Activity Trace ***IOCP System Configuration *MASPZAP Data Management ADRDSSU DASD Management AMAZAP Data Management BLSROPTR Data Management DEBE Data Management DITTO Data Management FDRZAPOP Product Internal ICKDSF DASD Management IDCSC01 IDCAMS Set Cache IEHATLAS Data Management IEHD**** DASD Management IEHINITT Tape Management IFASMFDP SMF Data Dump IGWSPZAP Data Management IND$FILE PC to Mainframe *****SCP System Configuration		
	DATA SET CONTROLS			
85.	Are all data set rules appropriately protected?	All data set rules should be appropriately protected.		
86.	Is global access to data sets used on data set rules restricted at the appropriate level of access?	Global access on data sets should be restricted to the appropriate level of access for general purpose libraries.		
87.	Is the UACC (Universal Access) for all Data Set profiles defined as NONE?	The UACC (Universal Access) for all Data Set profiles should be defined as NONE.		
88.	For data sets requiring global access, is the PERMIT(*) command utilized?	For data sets requiring global access the PERMIT(*) command should be utilized. This allows for only IDS defined to the security software to access the data set.		
	VOLUME CONTROLS			
89.	Is the DASDVOL resource class used to restrict VOLUMES?	The DASDVOL resource class should be used to restrict VOLUMES.		
90.	Is the DASDVOL resource defined as a UACC(NONE)?	The DASDVOL resource should be defined as a UACC(NONE).		
	SENSITIVE UTILITY CONTROLS Utilities are essential to data center operations and support. Tape Management, DASD Management, Job Scheduling, Storage Alteration, System Modification			
91.	Are sensitive utility controls defined under the RACF resource class PROGRAM?	Sensitive utility controls should be defined under the RACF resource class PROGRAM.		
92.	Is access to sensitive utilities appropriately defined?	Access to sensitive utilities should be appropriately defined.		
93.	Are the resources relating to	Access to the resources relating to		

Step #	Procedure Description RACF RESOURCE CONTROLS	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
	sensitive utilities appropriately controlled and defined?	sensitive utilities should be appropriately controlled and defined.		
94.	Are accesses to the resource audited by the system?	Accesses to the resource should be audited by the system.		
	DYNAMIC LIST CONTROLS			
95.	Are generic and specific resource rules defined to prevent access by default?	Generic and specific resource rules should be defined on the system to prevent access by default system settings.		
96.	Are all accesses to the resource logged by the system?	Accesses to the resource should be logged by the system.		
97.	Is access to the resource limited to only authorized personnel?	Access to the resource should be limited to only authorized personnel.		
98.	Are dynamic list controls defined under the FACILITY resource class?	Dynamic list controls should be defined under the FACILITY resource class.		
	CONSOLE CONTROLS Consoles are protected via resources in the CONSOLE, FACILITY, OPERCMDS, and TSOAUTH resource classes. Console controls allow an installation to restrict access to operator consoles and allow a secure replacement of various 3rd party console facilities.			
99.	Are MCS Console controls defined under the RACF resource classes: CONSOLE, OPERCMDS, TSOAUTH?	MCS Console controls should be defined under the RACF resource classes: CONSOLE, OPERCMDS, TSOAUTH.		
100.	Are the user or group profiles for each real MCS Console granted READ access to the associated MCS console resource?	The user or group profiles for each MCS Console should be granted READ access to the associated MCS console resource.		
101.	Are the user or group profiles for operators and system programmers granted READ access to the associated MCS console resource?	The user or group profiles operators and system programmers should be granted READ access to the associated MCS console resource.		
	OS/390 SYSTEM COMMAND CONTROLS			
102.	Are OS/390 system commands controls defined under the OPERCMDS resource class?	OS/390 system commands controls should be defined under the OPERCMDS resource class.		
103.	Are accesses to these resources logged by the system?	Accesses to the resource should be logged by the system.		

Comments:
Action Plan:

Test Number: **5**	SITE:	DATE:	TIME:
Test Name: **TOP SECRET RESOURCE CONTROLS**			
Resources Required:	Mainframe Terminal Access		
Personnel Required:	System Programmers/Security Administrator		
Objectives:	Review of Top Secret Resource Controls		
Procedure Description: (Summary)	Verify that the Top Secret resource controls are configured to meet USDA policies and requirements.		

Detailed Procedures and Results

Step #	Procedure Description TOP SECRET RESOURCE CONTROLS	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
	GLOBAL OPTIONS Parameter and Description	**DEFAULT SETTINGS**		
1.	**ADABAS** Controls SVC numbers used by ADABAS at startup. Only valid for ADABAS 4.8 and 4.9.	Site defined		
2.	**ADMINBY** Enables administration information to be recorded for security changes.	ADMINB		
3.	**ADSP** Controls global automatic data set protection.	ALL (default) YES (MVS Version 1.x NO (MVS Version 2.x and above) *NOTE: Setting is also dependent on the type(s) of catalogs in use on the system.*		
4.	**AUTH** Controls authorization checking.	OVERRIDE, ALLOVER		
5.	**AUTOERASE** Controls auto-erase feature necessary to meet NCSC requirements.	Unclassified Systems: Optional Classified Systems: YES *CAUTION: Usage will affect performance.*		
6.	**BACKUP** Controls automatic Security File backup.	Site defined		
7.	**BYPASS** Specifies jobs and started tasks that bypass security in an emergency.	As applies to a specific system *NOTE: Local changes should be justified in writing with supporting documentation.*		
8.	**CANCEL** Allows TOP SECRET to be	NO		

Step #	Procedure Description TOP SECRET RESOURCE CONTROLS	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
	canceled via the operating system CANCEL command.			
9.	**CPF** Controls startup of Command Propagation Facility.	Site defined		
10.	**CPFNODES** Identifies remote nodes to which TSS commands can be transmitted.	Site defined, (*) *Note: This parameter is affected by NODES CPF.*		
11.	**CPFRCVUND** Identifies whether or not the local node can receive commands transmitted from remote nodes that have not been defined to the CPFNODES list.	NO		
12.	**CPFTARGET** Controls default for TSS command TARGET keyword.	Site defined		
13.	**CPFWAIT** Controls default for TSS command WAIT keyword.	YES		
14.	**DATE** Sets date display format.	MM/DD/YY		
15.	**DB2FAC** Controls protection of DB2 subsystems. New option under Release 4.4.	Site defined		
16.	**DEBUG** Controls debugging feature. Use as directed by CA support.	OFF		
17.	**DIAGTRAP** Controls diagnostic traps. Use as directed by CA support.	OFF		
18.	**DL1B** Controls protection of DBD and PSB for DL/1 batch programs.	NO		
19.	**DOWN** Controls action taken when TSS address space is inactive.	SB, BW, OW, and either: TW (if users are still defined in SYS1.UADS) **- or -** TN (if only systems personnel remain defined in SYS1.UADS		
20.	**DRC (Detail Reason Codes)** Modifies or lists particular DRC attributes.	As applies to a specific system		
21.	**DUFPGM** Identifies programs allowing for extraction or upgrade of INSTDATA.	As applies to a specific system		
22.	**DUMP** Takes formatted dumps of TSS address space.	As applies to a specific system and depends on version level *Note: Used for diagnostics*		

Step #	Procedure Description TOP SECRET RESOURCE CONTROLS	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
23.	**EXIT** Installation user exit.	ON		
24.	**EXPDAYS** Specifies the number of days that a PERMIT or ADD is held in the Security File before deletion.	0		
25.	**FACILITY** Controls facility processing.	As applies to general control options for the system. Examples: TSO BATCH IDMS CICS PROGRAM *Note: Refer to CA-Top Secret Manual.*		
26.	**HPBPW** Days to honor previous batch password	1-3 days		
27.	**INACTIVE** Controls users who have been inactive for a specific period.	35 days maximum		
28.	**IOTRACE** Controls TSS I/O trace.	OFF		
29.	**JCT** Identifies JES2 JCT offsets.	As applies to a specific system *Note: Refer to CA-Top Secret Manual.*		
30.	**JES** Identifies JES2/JES3 subsystems.	NOVERIFY		
31.	**JOBACID** Controls ACID identification for batch jobs.	Site defined by the ISSO		
32.	**LOG** Controls incident recording for all facilities.	MSG, SEC9, INIT, SMF		
33.	**LOGBUF** Allows the maximum number of in-core logging buffers to be used.	32		
34.	**MODE** Controls processing mode for all facilities.	FAIL		
35.	**MSG** Alters characteristics of TSS violation messages.	As applies to a specific system *NOTE: Local changes should be justified in writing with supporting documentation.*		
36.	**MSUSPEND** Allows Master Security Control ACID (MSCA) to be suspended	YES		

Step #	Procedure Description TOP SECRET RESOURCE CONTROLS	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
	if password violation occurs.			
37.	**NEWPW** Selects new password specification rules.	MIN=6, MINDAYS=1, RS, ID, WARN=10, NR=0, TS		
38.	**NJEUSR** Defines a default ACID for NJE Store-and-Forward nodes. Has no significance on a job's execution node.	NJEUSER(NJESTORE)		
39.	**NPWRTHRESH** Sets maximum threshold, from 0 to 99, for new passwords to be verified before the complete logon sequence needs restarting.	2		
40.	**OPTIONS** This parameter is used to control optional APARs that have been applied prior to Release 5.1	Site defined *NOTE: Local changes should be justified in writing with supporting documentation.*		
41.	**PRODUCTS** Specifies special products installed.	TSO/E As applicable to the individual sites *NOTE: Local changes should be justified in writing with supporting documentation.*		
42.	**PTHRESH** Specifies password violation threshold.	2		
43.	**PWEXP** Specifies password expiration interval.	90		
44.	**PWHIST** Specifies number of previous passwords to be maintained in history file.	10		
45.	**PWVIEW** Controls display of passwords by administrators.	NO		
46.	**RECOVER** Controls change recovery.	ON *NOTE: Requires the RECFILE DD statement in the TSS STC.*		
47.	**REINIT** Requests that TOP SECRET re-initialize its internal control blocks and modules.	Site defined		
48.	**RESETEOD** Allows TOP SECRET to be restarted, without *IPLing*, after it has been brought down accidentally.	Site defined		
49.	**RESETSTATS** Used to reset all counters	Site defined		

Step #	Procedure Description TOP SECRET RESOURCE CONTROLS	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
	displayed by the STATS control option to zero (**0**).			
50.	**RPW** Allows the site to modify and list the contents of the Restricted Password list.	Site defined		
51.	**SECTRACE** Controls security diagnostic trace.	OFF *NOTE: May be activated on an as-needed basis, only for diagnostic purposes.*		
52.	**SUBACID** Controls on-line job submission.	U, 7		
53.	**SUSPEND** Allows an operator to suspend any ACID.	Site defined		
54.	**SVCDUMP** Produces a system dump of the TSS region.	Site defined		
55.	**SWAP** Controls TSS address space swapping.	NO		
56.	**SYNC** Requests immediate synchronization of global in-memory tables with the Security File. Only required for processors in global DORMANT mode.	Site defined		
57.	**SYSOUT** Spins off TSS activity log; specifies class and destination.	X, LOCAL		
58.	**TAPE** Controls tape processing.	OFF *NOTE: OFF indicates that an External Tape Management System (ETMS) is in use.*		
59.	**TEMPDS** Controls temporary data set protection.	YES		
60.	**TEXTTSS** Identifies up to 19 characters to replace the string, *CA-TOP SECRET SECURITY*, in messages and reports.	As applies to a specific system		
61.	**TIMER** Interval at which data is written from TSS buffers to AUDIT/TRACKING file.	30		
62.	**TSS** Allows the TOP SECRET administrator to enter TSS commands at the OS console	Site defined		
63.	**VMJESLNK** Causes any job submitted from the designated VM node(s) to	Site defined		

Step #	Procedure Description TOP SECRET RESOURCE CONTROLS	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
	be assigned an ACID equal to that of the VM submitter.			
64.	**VTHRESH** Selects violation threshold and action.	10, NOT, CAN		
	USER Profile Settings **A sample of user ids should be verified.**			
	User Profile Parameter and Description	**DEFAULT SETTINGS**		
65.	**FAC** Facilities the user is validated to use	Examples: BATCH -For batch users TSO - For TSO users NC-PASS For highly privileged users controlled by NC-PASS. Other - As necessary		
66.	**NAME(username)** Specifies the 1- to 20-character name of the user.	Field should be completed for all users		
67.	**PASSWORD** The logon password for the user	Field should be completed for all users		
68.	**INSTDATA** Installation-defined data	Optional		
69.	**PROF** Profile(s) defining the user's attributes	Field should be completed for all users		
70.	**TSOACCT** Specifies the user's TSO logon account. Used for all billing.	May be required for support. Only applicable if not using UADs.		
71.	**TSOLACCT** Specifies the user's default TSO logon account. Used for all billing.	May be required for support		
72.	**TSOAUTH** Used to secure TSO user attributes	Field should be completed for all TSO users		
73.	**TSOLPROC** Specifies the user's default TSO logon procedure	Field should be completed for all TSO users		
74.	**TSOPROC** Specifies the user's TSO logon procedure	Field should be completed for all TSO users		
	SPECIAL PROCESSING IDS for Business Applications, Administration, and system support functions			
	Batch Processing IDs			
75.	Are Batch Processing IDs established as default IDs on the system?	Batch Processing IDs should not be established as default IDs on the system.		
76.	Are Batch Processing IDs established with only minimum	Batch Processing should only be established with minimum authority		

Step #	Procedure Description TOP SECRET RESOURCE CONTROLS	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
	authority on the system necessary to perform its function?	on the system necessary to perform its function.		
77.	Are Batch Processing IDs distinguished from the general TSO user IDs on the system?	Batch Processing IDs should be distinguished from the general TSO user IDs on the system.		
78.	Are submissions for Batch Processing IDs using a job scheduler?	Batch submissions should be using a job scheduler.		
	Started Task Control IDs			
79.	Are Started Task IDs established as default IDs on the system?	Started Task IDs should not be established as default IDs on the system.		
80.	Are Started Task IDs established with only minimum authority on the system necessary to perform its function?	Started Task IDs should only be established with minimum authority on the system necessary to perform its function.		
81.	Are Started Tasks assigned a unique TYPE=USER ACID?	Started Tasks should be assigned a unique TYPE=USER ACID.		
82.	Are Started Task IDs defined with the STC facility?	Started Task IDs should be defined with only the STC facility.		
83.	If Started Task IDs require the capability to submit batch jobs, is the Started Task IDs granted FAC(BATCH)?	If Started Task IDs require the capability to submit batch jobs, the Started Task IDs should be granted FAC(BATCH). However, this will allow the STC itself to be executed as a batch job.		
84.	Do Started Tasks not defined to TSS fail upon initiation?	Started Tasks not defined to TSS should fail upon initiation.		
85.	Are Started Task defined to the STC table?	Started Task should be defined to the STC table.		
86.	Are Started Tasks granted NOSUSPEND privilege to exempt a Started Task associated ID from suspension for excessive violations? An STC can be canceled for excessive violations.	Started Tasks should be granted NOSUSPEND privilege to exempt a Started Task associated ID from suspension for excessive violations.		
	Storage Management IDs			
87.	Are Storage Management IDs established as default/generic IDs on the system?	Storage Management IDs should not be established as default/generic IDs on the system.		
88.	Are Storage Management IDs established with only minimum authority on the system necessary to perform its function?	Storage Management IDs should only be established with minimum authority on the system necessary to perform its function.		
89.	Are Storage Management IDs distinguished from the general TSO user IDs on the system?	Storage Management IDs should be distinguished from the general TSO user IDs on the system.		
90.	Are Storage Management IDs defined to the BATCH facility?	Storage Management IDs should be defined to the BATCH facility.		
	Emergency IDs			
91.	Are there separate emergency	There should be separate		

Step #	Procedure Description TOP SECRET RESOURCE CONTROLS	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
	IDs to perform operating and administrative functions on the system?	emergency IDs to perform operating and administrative functions on the system.		
92.	Are the activities from the emergency IDs logged on the system?	All activities from the emergency IDs should be logged on the system.		
93.	Are there documented procedures for the use and release of the emergency IDs?	There should be documented procedures for the use and release of emergency IDs.		
94.	Are Emergency IDs capable security administration (MSCA) stored appropriately?	Emergency IDs capable security administration (MSCA) should be stored appropriately.		
	FTP IDs			
95.	Is Anonymous FTP disabled on the system?	Anonymous FTP should be disabled on the system.		
96.	Are all scripts and/or data files located on the remote(s) that contain the MVS FTP ID and/or password secured and limited to only authorized personnel requiring access?	Secure all scripts and/or data files located on the remote system(s) that contain the MVS FTP ID and/or password (e.g., another OS/390 host or a remote UNIX system). Restrict access to these files to those individuals responsible for the application connectivity and who have a legitimate requirement to know the FTP ID and password.		
97.	Are the FTP IDs defined for only one system or application function?	FTP IDS should be defined for only one system or application function to prevent exposures to other systems.		
98.	Are the activities of the FTP IDS logged on the system?	All activities of the FTP IDS should be logged on the system.		
99.	Are FTP IDs established with only minimum authority on the system necessary to perform its function?	FTP IDs should only be established with minimum authority on the system necessary to perform its function.		
100.	Are FTP IDs established without TSO?	FTP IDs should be established without TSO.		
101.	Are FTP IDs established with non-expiring passwords?	FTP IDs should be established with non-expiring passwords. This is with the understanding that the application owner or group accepts the potential risks to the system.		
	MCS (Multiple Console Support) Console IDs MCS consoles allow operators to enter MVS and JES system commands.			
102.	Are MCS Console IDs defined without TSO or other online privileges?	MCS Console IDs should not be define with TSO or online privileges not required for the operation console.		
103.	Is the only resource MCS Console IDs permitted to access MVS.MCSOPER.consolename?	MCS Console IDs should not be permitted access to any resources except MVS.MCSOPER.consolename.		

Step #	Procedure Description TOP SECRET RESOURCE CONTROLS	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
104.	Are MCS Console controls defined under the resource classes: CONSOLE, OPERCMDS, TSOAUTH?	MCS Console controls should be defined under the resource classes: CONSOLE, OPERCMDS, TSOAUTH.		
105.	Are the group profiles for each real MCS Console granted READ access to the following commands: CONTROL, DISPLAY, MONITOR, STOPMN, STOPTR, TRACK?	The group profiles for each real MCS Console should be granted READ access to the following commands: CONTROL, DISPLAY, MONITOR, STOPMN, STOPTR, TRACK.		
106.	Are MCS Console IDS defined without TSO?	MCS Console IDS should be defined without TSO.		
	OS/390 System Operator IDS			
107.	Does each system operator have their own personal system operator ID?	Each system operator should have their own personal system operator ID.		
108.	If there are several system operators requiring access, is a TSS group defined and the system operators connected to the group?	If there are several system operators requiring access, a TSS group should be defined and the system operators connected to the group.		
109.	Are accesses to these resources logged by the system?	Accesses to these resources should be logged by the system.		
	SPECIAL PRIVILEGES			
	Modification Privileges			
	System and Administrator Privileges	Examples: MSCA SCA LSCA ZCA VCA DCA CONSOLE		
110.	Is the ***NOATS*** parameter assigned to all security administration IDs?	The ***NOATS*** parameter should be assigned to all security administration IDs.		
111.	Is authority to privileged access on the system limited to authorized personnel?	Authority to privileged access on the system should be limited to authorized personnel.		
112.	Is authority to privileged access on the system logged and reviewed/monitored routinely?	Authority to privileged access on the system should be logged and reviewed/monitored routinely.		
	Tape Label Bypass Privileges			
113.	Is access to Tape Label Bypass privileges restricted to authorized personnel?	Tape Label Bypass privileges should be restricted to only authorized personnel.		
114.	Is the Tape Label Bypass privilege controlled at the user level and not by the tape management system?	Tape Label Bypass privileges should be controlled at the user level and not by the tape management system.		
	Other Sensitive Privileges			
115.	Are Device Mount privileges	Device Mount privileges should be		

Step #	Procedure Description TOP SECRET RESOURCE CONTROLS	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
	restricted to authorized personnel?	restricted to authorized personnel.		
116.	Are TSOAUTH privileges for OPER and ACCOUNT restricted to authorized personnel?	TSOAUTH privileges for OPER and ACCOUNT should be restricted to authorized personnel.		
117.	Are sensitive commands that a TSO user can issue restricted?	TSO users should be restricted from issuing sensitive commands.		
118.	Is the ability to execute privileged programs restricted on the system?	The ability to execute privileged programs should be restricted on the system. Privileged Programs such as: ***GTF** System Activity Trace ***IOCP System Configuration *MASPZAP Data Management ADRDSSU DASD Management AMAZAP Data Management BLSROPTR Data Management DEBE Data Management DITTO Data Management FDRZAPOP Product Internal ICKDSF DASD Management IDCSC01 IDCAMS Set Cache IEHATLAS Data Management IEHD**** DASD Management IEHINITT Tape Management IFASMFDP SMF Data Dump IGWSPZAP Data Management IND$FILE PC to Mainframe *****SCP System Configuration		
119.	Is the TSO/E CONSOLE facility restricted to authorized personnel?	The TSO/E CONSOLE facility should be restricted to authorized personnel.		
120.	Is the AUDIT turned on for users who have CONSOLE attribute?	Audit should only be turned on if there is suspected wrongdoing.		
121.	Is the Trace attribute only used for trouble shooting purposes?	Trace attribute should only be used for trouble shooting purposes.		
122.	Is the NOxxxCHKs bypass attribute strictly controlled?	The NOxxxCHKs bypass attribute should be strictly controlled.		
123.	Is the FAC(ALL) access strictly controlled?	Access to all facilities FAC(ALL) should rarely be granted.		
124.	Is the NOSUSPEND privilege granted to any ID on the system?	NOSUSPEND privilege should not be granted to any ID.		
	DATA SET CONTROLS			
125.	Are all data set rules appropriately protected?	All data set rules should be appropriately protected.		
126.	Prior to the inclusion to ALL RECORD, is the access level reviewed, and restricted at the appropriate level?	Global access on data sets should be restricted to the appropriate level of access for general purpose libraries.		
	VOLUME CONTROLS			
127.	Is blanket access or	Blanket access or permissions to		

Step #	Procedure Description TOP SECRET RESOURCE CONTROLS	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
	permissions to volumes should not be allowed on the system?	volumes should not be allowed on the system.		
128.	Are Volumes defined by valid prefixes or discrete volume names for each OS/390 domain, this Is to include DASD volumes.	Volumes should be defined by valid prefixes or discrete volume names for each OS/390 domain; this Is to include DASD volumes as well.		
	SENSITIVE UTILITY CONTROLS Utilities are essential to data center operations and support. Tape Management, DASD Management, Job Scheduling, Storage Alteration, System Modification			
129.	Are the resources relating to sensitive utilities appropriately controlled and defined?	Access to the resources relating to sensitive utilities should be appropriately controlled and defined.		
130.	Is access to data sets in which sensitive utilities reside restricted?	Access to data sets in which sensitive utilities reside should be restricted.		
131.	Are accesses to the resource audited by the system?	Accesses to the resource should be audited by the system.		
132.	Are sensitive utilities defined and controlled by the PROGRAM protection authorization?	Sensitive utilities should be defined and controlled by the PROGRAM protection authorization.		
	DYNAMIC LIST CONTROLS			
133.	Are generic and specific resource rules defined to prevent access by default?	Generic and specific resource rules should be defined on the system to prevent access by default system settings.		
134.	Are all accesses to the resource logged by the system?	Accesses to the resource should be logged by the system.		
135.	Is access to the resource limited to only authorized personnel?	Access to the resource should be limited to only authorized personnel.		
136.	Are dynamic list controls defined under the FACILITY resource class?	Dynamic list controls defined under the FACILITY resource class.		
	CONSOLE CONTROLS Consoles are protected via resources in the CONSOLE, FACILITY, OPERCMDS, and TSOAUTH resource classes. Console controls allow an installation to restrict access to operator consoles and allow a secure replacement of various 3rd party console facilities.			
137.	Are MCS Console controls defined under the resource classes: SYSCONS, OPERCMDS, TSOAUTH?	MCS Console controls should be defined under the resource classes: SYSCONS, OPERCMDS, TSOAUTH.		
138.	Is the user or group profiles for each real MCS Console granted READ access to the associated console resource?	The user or group profiles for each real MCS Console granted READ access to the associated console resource.		
139.	Are the user or group profiles	The user or group profiles for each		

Step #	Procedure Description TOP SECRET RESOURCE CONTROLS	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
	for each real MCS Console granted READ access to the associated MCS console resource?	MCS Console should be granted READ access to the associated MCS console resource.		
	OS/390 SYSTEM COMMAND CONTROLS			
140.	Are OS/390 system commands controls defined under the OPERCMDS resource class?	OS/390 system commands controls should be defined under the OPERCMDS resource class.		
141.	Are accesses to these resources logged by the system?	Accesses to these resources should be logged by the system.		
	TOP SECRET ENCRYPTION KEY			
142.	Is the encryption key recorded and locked in an acceptable container in the event that the encryption key is required?	The encryption key should be recorded and locked in an acceptable container in the event that the encryption key is required		
143.	Are only authorized personnel allowed to access the container?	Only authorized personnel allowed to access the container.		
144.	The encryption key resides in a linklist load library. Is access to this library restricted to only Security or Systems personnel?	Access to this library restricted to only Security or Systems personnel.		
145.	Are backup copies of the linklist load library protected and only authorized personnel has access?	Backup copies of the linklist load library should be protected and only authorized personnel should have access.		
146.	Is the source used to create the LNKLST load module restricted?	The source used to create the LNKLST load module should be restricted to authorized personnel.		
147.	Is the encryption key removed from the source after load?	The encryption key should be removed from the source after load.		

Comments:
Action Plan:

Test Number: **6**	SITE:	DATE:	TIME:
Test Name**: NETWORK COMMUNICATION**			
Resources Required:	Mainframe Terminal Access		
Personnel Required:	Systems Programmer/Security Administrator		
Objectives:	Review of Network Communication		
Procedure Description: (Summary)	Verify that the network communication resource controls are configured to meet USDA policies and requirements.		

Detailed Procedures and Results

Step #	Procedure Description Network Communication	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
	TCP/IP CONSIDERATIONS			
1.	Are the TCP/IP resources established with the necessary controls to protect the mainframe environment and routinely audited?	TCP/IP resources should be established with the necessary controls to protect the mainframe environment and routinely audited. Examples: TCP userids SERVAUTH Class • Stack Access • Net Access • Port Access • Netstat Access • TN3270 File FTP.DATA (ddname sysftpd) File TCPIP.DATA (ddname systcpd) • DATASETPREFIX parameter • Hostname to match standard NJE name for host. File PROFILE.TCPIP (DDNAME PROFILE) • PORT parameter values 0-1023 are to be maintained. • PORT parameter values 1024 – 65535 • POOL SIZE Parameters • DATASETPREFIX parameter • Logmode specification for BEGINVTAM Parameter		
2.	Are the TCP/IP resources established on the servers	TCP/IP resources should be established on the servers with the		

Step #	Procedure Description Network Communication	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
	with the necessary controls to protect the mainframe environment and routinely audited?	necessary controls to protect the mainframe environment and routinely audited. Examples: Communications servers FTP servers Print servers LDAP servers DCE Security servers UNIX System Services		
3.	Are system TCP/IP User ID connections properly authenticated on the system?	System TCP/IP User ID connections should be properly authenticated on the system.		
4.	Are end-user TCP/IP User ID connections properly authenticated on the system?	End-user TCP/IP User ID connections should be properly authenticated on the system.		
5.	Are IP addresses and their aliases secured on the system?	IP addresses and their aliases should be secured on the system?		
	VTAM SECURITY STANDARDS			
6.	Are logons from secure terminals defined with the USSTAB OR LOGAPPL definitions?	Use **USSTAB** or **LOGAPPL** definitions to control logon from secure terminals. These terminals can log on directly to any VTAM application (e.g., TSO, CICS, etc.) of their choice and bypass Session Manager services. The VTAM SME may be implemented to secure access to network resources because the use of **USSTAB** and **LOGAPPL** is not effective or is not possible in some cases.		
7.	Are secure terminals attached to the host or connected to the host via secure encrypted / dedicated lines?	Secure terminals are usually locally attached to the host or connected to the host via secure encrypted / dedicated lines.		
8.	Are only authorized personnel allowed to enter the area where the secure terminals are located?	Only authorized personnel should be able to enter the area where secure terminals are located.		
9.	Are unsecured terminals defined with the LOGAPPL definitions? Dial-up terminals or terminals attached to the Internet (e.g., TN3270 terminals, emulation terminals) are examples of unsecured terminals.	Use **LOGAPPL** definitions for all unsecured terminals. These terminals must first establish a session with the Session Manager (e.g., CL/GATEWAY, Netmaster) before establishing connectivity with any other VTAM application (e.g., TSO, CICS) in the host.		
10.	Are users identified before any session can be	The user should be identified before any session is allowed for the system.		

Step #	Procedure Description Network Communication	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
	established for the system?			
11.	Are there any vendor's default installation /configuration options installed on the system that bypasses the Session Manager services?	Use of any vendor's default installation / configuration option that bypasses Session Manager services should not be installed on the system.		
12.	Does the Session Manager perform security verification (such as I&A), and only show the applications the user is authorized to access?	The Session Manager should perform security verification (such as I&A), and should only show the applications the user is authorized to access.		
13.	Does the Session Manager have a SAF or equivalent interface with the security software such as ACF2, RACF, or TOP SECRET?	The Session Manager should have an SAF or equivalent interface with Security software such as ACF2, RACF, or TOP SECRET.		
14.	Does the Session Manager or VTAM display a legal notification banner?	The Session Manager or VTAM (via **USSTAB MSG10**) should display a legal notification banner.		
15.	Are accesses controlled to to all VTAM system data sets, all VTAM load modules and exit routines, and all VTAM start options and definition statements by the services of a security software?	Control access to all VTAM system data sets, all VTAM load modules and exit routines, and all VTAM start options and definition statements by the services of a security software.		
16.	Are accesses to the VTAM system resources restricted to only authorized personnel?	Accesses to the VTAM system resources should be restricted to only authorized personnel.		
17.	Has the SMETAB been coded properly?	The SMETAB should be coded with the following:		
	SME: Session Management Exit	Code operand **CLSDST=Y** in the AUTHTAB macro to allow the Session Manager to initiate logons to VTAM applications selected by terminal users from the selection menu. **CLSDST-PASS** processing is a way to tell VTAM that the user has been verified by the Session Manager and that application access is authorized.		
		Code ACCEPT macros for authorized sessions between LUs representing network terminals and the Session Manager.		
		Code ACCEPT macros for any pair of LUs (all types of LUs including LU 6.2) authorized to establish sessions with each other. LUs may be in the same network (same net ID) or in		

Step #	Procedure Description Network Communication	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
		interconnected networks (different net ID).		
		Code REJECT macros for any pairs of LUs (all types of LUs including LU 6.2) that are **not authorized** to establish sessions with each other. LUs may be in the same network (same net ID) or in interconnected networks (different net ID).		
		Code the **TWOWAY** operand in ACCEPT and REJECT macros only if bi-directional session authorization or rejection is necessary.		
		Use generic entries wherever possible To reduce the number of entries in the **SMETAB**, and to improve SME performance during session pair authorization.		
		Code a REPORT macro to generate SMF records to provide an audit trail		
18.	Are naming standards established for network resources to take the best advantage of the services of the SME (Session Management Exit)?	Naming standards should clearly distinguish between host applications and remote devices, between physically secured and unsecured terminals, and between sensitive and general access applications.		
19.	Is encryption used to protect sensitive, classified or confidential data transmitted between network end points, and to prevent unauthorized personnel from reading or modifying the data being transferred.	Wherever possible, encryption should be used to protect sensitive, classified or confidential data (e.g., passwords) transmitted between network end points, and to prevent unauthorized personnel from reading or modifying the data being transferred. Selected encryption implementations should comply with established NSA standards.		
	LU 6.2 (APPC) APPLICATIONS			
20.	Is the LU 6.2 session-level LU-LU verification used to verify the identity of each partner LU during the activation of sessions between LU 6.2 applications?	The LU 6.2 session-level LU-LU verification should be used to verify the identity of each partner LU during the activation of sessions between LU 6.2 applications. Under this verification mechanism, one LU-LU password is assigned to each LU pair.		
21.	Are unique passwords used only as a cryptography key to encrypt/decrypt random data exchanged between the LU partners at session establishment?	Unique passwords should be used only as a cryptography key to encrypt / decrypt random data exchanged between the LU partners at session establishment. If all LU-LU verifications are successful, the session can be established between the LU pair.		
22.	Is the LU 6.2 userid verification utilized?	Utilize LU 6.2 userid verification. This is because user verification, using the Session Manager, is generally not		

Step #	Procedure Description Network Communication	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
		available for LU 6.2 applications. Under this verification mechanism, VTAM allows an LU to send the userid and password in the request to establish a conversation so that the partner LU can verify them.		
23.	Is the SME used for LU 6.2 Session control between two LU 6.2 applications?	The SME for LU 6.2 session control between two LU 6.2 applications.		
	FRONT END PROCESSORS (FEPs) FEPs are intermediate nodes located between the OS/390 hosts and the remote network devices. They do not process data but they receive, buffer and then pass data through the network.			
24.	Is access to the service subsystem functions and FEP resources from the control panel and from FEP console (local or remote) enforced and restricted only to authorized personnel?	Access to service subsystem functions and FEP resources from the control panel and from FEP console (local or remote) should be enforced and restricted only to authorized personnel.		
25.	Is permission to change passwords restricted to the minimum number of authorized personnel?	Control authorization to use service subsystem console (local or remote) by FEP internal security control through password validation. Restrict access to these passwords to the absolutely minimum number of necessary personnel.		
26.	Are vendor default passwords utilized on the system?	Use of vendor default passwords should not be used on the system.		
27.	Are different passwords assigned for local and remote FEP consoles?	Different passwords should be assigned for the local and remote FEP consoles.		
28.	After three unsuccessful logon attempts, are the local/remote FEP consoles disconnected?	After three unsuccessful logon attempts, the local/remote consoles should be disconnected.		
29.	Are passwords used by vendor (COMTEN, IBM, CNT, or AMDAHL) service Personnel changed after any maintenance is completed?	Passwords used by vendor (COMTEN, IBM, CNT, or AMDAHL) service personnel should be changed after any maintenance is done		
30.	Is the key-lock switch used on the modem supporting the remote console of the service subsystem to prevent unauthorized access?	Use a key-lock switch on the modem supporting the remote console of the service subsystem to prevent unauthorized access. The key-lock switch is only open for scheduled and authorized remote access and removed after use.		
31.	Is access to the NCP system resources secured and access restricted to authorized personnel?	Control access to NCP system data sets, NCP source definition data sets, NCP load modules, and NCP dump data sets stored in the host by the		

Step #	Procedure Description Network Communication	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
		services of a security software. Restrict access only to authorized personnel.		
32.	Is access to the host support software programs secured and access restricted to authorized personnel?	Control access to host support software programs by the services of a security software. Restrict access only to authorized personnel. The host support software programs contain utilities that assemble, generate, load, and dump the NCP, and utilities to format and print NCP dumps.		
33.	Are only authorized personnel allowed to issue Load /Dump /Activate/ Deactivate NCP commands?	Only authorized personnel should issue Load /Dump /Activate/ Deactivate NCP commands.		
34.	Do authorized personnel use the VTAM display command and the services of the service subsystem to verify periodically the current valid version of the NCP load module (generation Date and time) and FEP disk contents?	Authorized personnel should use the VTAM display command and the services of the service subsystem to verify periodically the current valid version of the NCP load module (generation date and time) and FEP disk contents. The operators will report any unusual conditions to management immediately.		
35.	Are strict change control / management in place for any hardware upgrade or software change, FEP memory upgrade, installation of new communication lines, new release of NCP, and new NCPGEN to support additional support of remote devices by the NCP, etc. ?	Strict change control / management should be in place for any hardware upgrade or software change, FEP memory upgrade, installation of new communication lines, new release of NCP, and new NCPGEN to support additional support of remote devices by the NCP, etc. Explain and fully document any upgrade/change to the current version/configuration.		
36.	Are the current change control / management mechanisms reviewed to detect and eliminate potential security exposures?	The current change control /management mechanisms should be reviewed to detect and eliminate potential security exposures. Document any potential security exposures.		
37.	Are hardware and software upgrades / changes logged for auditing purposes and problem tracking?	Maintain a log of all hardware and software upgrades / changes for auditing purposes and problem tracking.		
	MQSeries MQSeries from IBM provides applications the ability to communicate with each other using messages and queues. This message-driven processing enables any-platform-to-any-platform communication.			
38.	Is user access restricted to resources necessary to accomplish their assigned responsibilities?	Restrict user access to resources necessary to accomplish their assigned responsibilities. These resources include, but are not limited to, MQSeries objects, programs, and data sets.		

Step #	Procedure Description Network Communication	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
39.	Is the installation and maintenance of the MQSeries performed via SMP/E?	MQSeries installation and maintenance should be performed via SMP/E.		
	CHANNEL SECURITY EXITS			
40.	Do exits authenticate with a unique userid and a password for each channel?	The exits should authenticate with a unique userid and a password for each channel.		
41.	Are the channel security exits defined for both ends of the channel?	The channel security exits work in pairs. Ensure that compatible exits are named for both ends of the channel.		
42.	Is the name of the channel security exit defined in the SCYEXIT parameter?	The name of the channel security exit should be defined in the SCYEXIT parameter of the channel definition.		
43.	Does the channel security exit module for distributed queues not involving CICS reside in the data set specified by the CSQXLIB DD of the channel initiator procedure?	For distributed queues not involving CICS, the channel security exit module should reside in the data set specified by the CSQXLIB DD of the channel initiator procedure.		
44.	Are channel security exits reviewed and approved prior to implementation in a production environment?	All Channel Security Exits should be reviewed and approved prior to implementation in a production environment.		
	Switch Profiles Switch profiles are special MQSeries profiles that turn off security checking for a type of resource.			`
45.	Are profiles with the first two qualifiers of ssid.NO defined to the MQADMIN class?	No profiles with the first two qualifiers of *ssid.NO* should be defined to the **MQADMIN** class, with the exception of *ssid.NO.CMD.RESC.CHECKS.*		
46.	Are all sensitive MQSeries commands restricted to queue managers, channel initiators, and designated systems personnel?	All sensitive MQSeries commands should be restricted to queue managers, channel initiators, and designated systems personnel.		
	Utilities			
47.	Are MQSeries programs restricted to the MQSeries administrator and systems programming personnel?	MQSeries programs should be restricted to the MQSeries administrator and systems programming personnel.		
48.	Are MQSeries programs defined to the **PROGRAM** class?	MQSeries programs should be defined to the **PROGRAM** class: CSQUTIL CSQUCVX CSQJU003 CSQJU004 CSQ1LOGP		
	Userid Timeouts			
49.	Are IDs signed on to a queue manager logged off after 15 minutes of	IDs signed on to a queue manager should be logged off after 15 minutes of inactivity. This timeout process		

Step #	Procedure Description Network Communication	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
	inactivity?	should be implemented by including the **ALTER SECURITY** command in the **CSQINP1** data set.		
	ACF2			
	Security Classes			
50.	Is ACF2 checking performed on all MQSeries resources?	The following CLASMAP records must be inserted in order for ACF2 checking to be performed. MQADMIN MQCONN MQCMDS MQQUEUE MQPROC MQNLIST		
	Started Tasks			
51.	Are started task IDs established for each queue manager started task procedure and distributed queuing started task procedure?	A started task id entry should be created for each queue manager started task procedure and distributed queuing started task procedure.		
52.	Is a corresponding userid established for each started task with the following LID parameters: STC, MUSASS, NOSMC	A corresponding userid should be established for each started task and should have the following LID parameters: STC, MUSASS, NOSMC		
	Datasets			
53.	Are the following data sets APF authorized: *hlqual*.SCSQAUTH *hlqual*.SCSQLINK *hlqual*.SCSQANLx *hlqual*.SCSQSNL *hlqual*.SCSQMVR1 *hlqual*.SCSQMVR2	The installation requires that the following data sets be APF authorized. *hlqual*.SCSQAUTH *hlqual*.SCSQLINK *hlqual*.SCSQANLx *hlqual*.SCSQSNL *hlqual*.SCSQMVR1 *hlqual*.SCSQMVR2		
54.	Is *Write* and *allocate* access to data set profiles protecting all page sets, logs, bootstrap data sets (BSDS), and data sets referenced by the CSQOUTX and CSQSNAP DDs in the queue manager's procedure restricted to the queue manager userid, MQSeries administrator, and systems programming personnel?	*Write* and *allocate* access to data set profiles protecting all page sets, logs, bootstrap data sets (BSDS), and data sets referenced by the CSQOUTX and CSQSNAP DDs in the queue manager's procedure should be restricted to the queue manager userid, MQSeries administrator, and systems programming personnel. Log all *write* and *allocate* access to these data sets.		
55.	Is *Allocate* access to all archive data sets in the queue manager's procedure restricted to the queue manager userid, MQSeries administrator, and systems programming personnel?	*Allocate* access to all archive data sets in the queue manager's procedure should be restricted to the queue manager userid, MQSeries administrator, and systems programming personnel. Log all *allocates* access to these data sets.		
	Connection Security			
56.	Is connection security	Connection security should be active		

Step #	Procedure Description Network Communication	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
	active and all profiles defined in the MQCONN class?	and all profiles should be defined in the **MQCONN** class.		
57.	Is access to the connection security profiles restricted?	Access to connection security profiles should be restricted using the following table as a guideline: *ssid*.BATCH - TSO IDs Batch job IDs *ssid*.CICS - CICS region IDs *ssid*.IMS - IMS region IDs *ssid*.CHIN - Channel initiator IDs		
58.	Is access logged by the system?	All access should be logged by the system.		
	Queue Security			
59.	Is Queue security active and all profiles defined in the MQQUEUE class?	Queue security should be active and all profiles should be defined in the **MQQUEUE** class.		
60.	Is the message queue access restricted to those IDs that require the ability to get messages from and put messages to queues?	Message queue access should be restricted to those IDs that require the ability to get messages from and put messages to message queues. The profile names for queue security are *ssid.queuename*, where *ssid* is the name of a MQSeries subsystem.		
61.	Is access authorization to the system queues restricted to the CSQUTIL utility, MQSeries operations and control panels, channel initiators, MQSeries software monitors, and CICS transactions?	Access authorization to system queues (those queue resources with a first qualifier of *system*) should be restricted to the CSQUTIL utility, MQSeries operations and control panels, channel initiators, MQSeries software monitors, and CICS transactions.		
62.	Is an alias queue defined to resolve the real dead-letter queue?	Undeliverable messages can be routed to a dead-letter queue. Two levels of access must be established for these queues. The first level allows applications, as well as some MQSeries objects, to put messages to this queue. The second level restricts the ability to get messages from this queue and protects sensitive data. This should be accomplished by defining an alias queue that resolves to the real dead-letter queue, but defines the alias queue with the attributes **PUT(ENABLED)** and **GET(DISABLED)**.		
63.	Is the ability to get messages from the dead-letter queue restricted to message channel agents (MCAs), CKTI (MQSeries-supplied CICS task initiator), channel initiators utility, and any automated application used for dead-	The ability to get messages from the dead-letter queue should be restricted to message channel agents (MCAs), CKTI (MQSeries-supplied CICS task initiator), channel initiators utility, and any automated application used for dead-letter queue maintenance.		

Step #	Procedure Description Network Communication	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
	letter queue maintenance?			
	Process Security Process security validates IDs authorized to issue MQSeries inquiries on process definitions.			
64.	Is Process security active and all profiles *ssid.processname* defined in the MQPROC class?	Process security should be active, and all profiles *ssid.processname* should be defined in the **MQPROC** class.		
65.	Is read access restricted to those IDs requiring access to make process inquires?	Read access should be restricted to those IDs requiring access to make process inquiries.		
	Namelist Security A Namelist is a MQSeries object that contains a list of queue names. Namelist security validates IDs authorized to inquire on namelists.			
66.	Is Namelist security active and all profiles ssid.namelist defined in the MQNLIST class?	Namelist security should be active, and all profiles *ssid.namelist* should be defined in the MQNLIST class.		
67.	Is access restricted to those IDs requiring access to make namelist inquiries?	Restrict access to those IDs requiring access to make Namelist inquiries.		
	Alternate Userid Security Alternate userid security allows access to be requested under another userid.			
68.	Is Alternate userid security active and all profiles *ssid.ALTERNATE.USER.alternateuserid* defined to the MQADMIN class?	Alternate userid security should be active, and all profiles *ssid.ALTERNATE.USER.alternateuserid* should be defined in the **MQADMIN** class.		
69.	Is access restricted to those IDs requiring access to alternate IDs?	Restrict access to those IDs requiring access to alternate IDs.		
	Context Security Context security validates whether a userid has authority to pass or set identity and/or origin data for a message.			
70.	Is Context security active and all profiles *ssid.CONTEXT* defined to the MQADMIN class?	Context security should be active and all profiles *ssid.CONTEXT* should be defined in the **MQADMIN** class, where *ssid* is the queue manager name.		
	Command Security Command security validates IDs authorized to issue MQSeries commands.			
71.	Is Command security active and all profiles defined to the MQCMDS class?	Command security should be active, and all profiles should be defined in the **MQCMDS** class.		
72.	Is access to the command security profiles restricted?	Restrict access to command security profiles using the following table:		
	Command	**Profile**		
	ALTER xxxxx	ssid.ALTER.xxxxx		
	ARCHIVE LOG	ssid.ARCHIVE.LOG		

Step #	Procedure Description Network Communication	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
	CLEAR QLOCAL	ssid.CLEAR.QLOCAL		
	DEFINE xxxxx	ssid.DEFINE.xxxxx		
	DELETE xxxxx	ssid.DELETE.xxxxx		
	DISPLAY xxxxx	ssid.DISPLAY.xxxxx		
	PING xxxxx	ssid.PING.xxxxx		
	RECOVER BSDS	ssid.RECOVER.BSDS		
	REFRESH xxxxx	ssid.REFRESH.xxxxx		
	RESET xxxxx	ssid.RESET.xxxxx		
	RESOLVE xxxx	ssid.RESOLVE.xxxxx		
	RESUME QMGR	ssid.RESUME.QMGR		
	RVERIFY SECURITY	ssid.RVERIFY.SECURITY		
	START xxxxx	ssid.START.xxxxx		
	STOP xxxxx	ssid.STOP.CHINIT		
	SUSPEND QMGR	ssid.SUSPEND.QMGR		
	RESLEVEL Security RESLEVEL security profiles control the number of IDs checked for API resource security.			
73.	Is RESLEVEL security active?	RESLEVEL security should not be implemented due to the following exposures and limitations: (1) RESLEVEL is a powerful option that can cause the bypassing of all security checks. (2) Security audit records are not created when the RESLEVEL profile is utilized. (3) If the WARNING option is specified on a RESLEVEL profile, no warning messages are produced.		
74.	Is a RESLEVEL profile defined for each queue manager and no user or groups specified on the access list?	To protect against any profile in the **MQADMIN** class, such as s*sid.***, resolving to a RESLEVEL profile, a *ssid.RESLEVEL* profile should be defined for each queue manager and no users or groups specified in the access list.		
	CICS Transaction Security MQSeries-supplied CICS transactions should be properly secured.			
75.	Is access to the CICS transactions restricted to the CICS regions and the MQSeries administrator?	Access to the following transactions should be restricted to CICS regions and the MQSeries administrator: CKAM CKTI CKQC CKBM CKRT CKCN CKSD CKRS CKDP CKDL CKSQ		
	RACF			
	Security Classes:			
76.	Is RACF checking performed on all MQSeries resources?	In order to ensure that RACF checking is performed on all MQSeries resources, the following RACF security classes must be activated:		

Step #	Procedure Description Network Communication	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
		MQADMIN GMQADMIN MQCONN MQCMDS MQQUEUE GMQQUEUE MQPROC GMQPROC MQNLIST GMQNLIST		
	Started Tasks			
77.	Are started task IDs established for each queue manager started task procedure and distributed queuing started task procedure?	A started task id entry should be created for each queue manager started task procedure and distributed queuing started task procedure.		
78.	Is a corresponding userid established for each started task?	A corresponding userid should be established for each started task.		
79.	Is a Queue manager and channel initiator started task defined without the Trusted attribute?	Queue manager and channel initiator started tasks should not be defined with the **TRUSTED** attribute.		
	Datasets			
80.	Are the following data sets APF authorized: *hlqual*.SCSQAUTH *hlqual*.SCSQLINK *hlqual*.SCSQANLx *hlqual*.SCSQSNL *hlqual*.SCSQMVR1 *hlqual*.SCSQMVR2	The installation requires that the following data sets be APF authorized. *hlqual*.SCSQAUTH *hlqual*.SCSQLINK *hlqual*.SCSQANLx *hlqual*.SCSQSNL *hlqual*.SCSQMVR1 *hlqual*.SCSQMVR2		
81.	Is *Read* access to data sets referenced by the CSQINP1, CSQINP2, and CSQXLIB DDs in the queue manager's procedure restricted to the queue manager userid, MQSeries administrator, and systems programming personnel?	*Read* access to data sets referenced by the CSQINP1, CSQINP2, and CSQXLIB DDs in the queue manager's procedure should be restricted to the queue manager userid, administrator, and systems programming personnel. Log all access to these data sets.		
82.	Is *Update* access to data set profiles protecting all page sets, logs, bootstrap data sets (BSDS), and data sets referenced by the CSQOUTX and CSQSNAP DDs in the queue manager's procedure restricted to the queue manager userid, MQSeries administrator, and systems programming personnel?	*Update* access to data set profiles protecting all page sets, logs,bootstrap data sets (BSDS), and data sets referenced by the CSQOUTX and CSQSNAP DDs in the queue manager's procedure should be restricted to the queue manager userid, MQSeries administrator, and systems programming personnel. Log all *update* and *alter* access to these data sets.		
83.	Is *Alter* access to all archive data sets in the queue manager's procedure restricted to the	*Alter* access to all archive data sets in the queue manager's procedure will be restricted to the queue manager userid, MQSeries administrator, and		

Step #	Procedure Description Network Communication	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
	queue manager userid, MQSeries administrator, and systems programming personnel?	systems programming personnel. Log all *alters* access to these data sets.		
	Connection Security Connection security validates IDs authorized to connect to queue managers.			
84.	Is connection security active and all profiles defined in the MQCONN class?	Connection security should be active and all profiles should be defined in the **MQCONN** class.		
85.	Is access to the connection security profiles restricted?	Restrict access to connection security profiles using the following table as a guideline: *ssid*.BATCH - TSO IDs Batch job IDs *ssid*.CICS - CICS region IDs *ssid*.IMS - IMS region IDs *ssid*.CHIN - Channel initiator IDs		
86.	Is access logged by the system?	All access should be logged by the system.		
	Queue Security Queue security validates IDs authorized to access message queues.			
87.	Is Queue security active and all profiles defined in the **MQQUEUE** or **GMQQUEUE** class with UACC(NONE) specified?	Queue security should be active, and all profiles should be defined in the **MQQUEUE** or **GMQQUEUE** class with UACC(NONE) specified.		
88.	Is the Message queue restricted to those IDs that require the ability to get messages from and put messages to message queues?	Message queue access should be restricted to those IDs that require the ability to get messages from and put messages to message queues		
89.	Is access authorization to system queues (those queue resources with a first qualifier of *system*) restricted to the CSQUTIL utility, MQSeries operations and control panels, channel initiators, MQSeries software monitors, and CICS transactions?	Access authorization to system queues (those queue resources with a first qualifier of *system*) should be restricted to the CSQUTIL utility, MQSeries operations and control panels, channel initiators, MQSeries software monitors, and CICS transactions.		
90.	Is an alias queue defined to resolve the real dead-letter queue?	Undeliverable messages can be routed to a dead-letter queue. Two levels of access must be established for these queues. The first level allows applications, as well as some MQSeries objects, to put messages to this queue. The second level restricts the ability to get messages from this queue and protects sensitive data.		

Step #	Procedure Description Network Communication	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
		This should be accomplished by defining an alias queue that resolves to the real dead-letter queue, but defines the alias queue with the attributes **PUT(ENABLED)** and **GET(DISABLED)**.		
91.	Is the ability to get messages from the dead-letter queue restricted to message channel agents (MCAs), CKTI (MQSeries-supplied CICS task initiator), channel initiators utility, and any automated application used for dead-letter queue maintenance?	The ability to get messages from the dead-letter queue should be restricted to message channel agents (MCAs), CKTI (MQSeries-supplied CICS task initiator), channel initiators utility, and any automated application used for dead-letter queue maintenance.		
	Process Security Process security validates IDs authorized to issue MQSeries inquiries on process definitions.			
92.	Is Process security active and all profiles *ssid.processname* defined in the **MQPROC** or **GMQPROC** class with UACC(NONE) specified?	Process security should be active, and all profiles *ssid.processname* should be defined in the **MQPROC** or **GMQPROC** class with UACC(NONE) specified.		
93.	Is *Read* access restricted to those IDs requiring access to make process inquiries?	*Read* access should be restricted to those IDs requiring access to make process inquiries.		
	Namelist Security A namelist is a MQSeries object that contains a list of queue names. Namelist security validates IDs authorized to inquire on namelists.			
94.	Is Namelist security active and all profiles s*sid.namelist* defined in the **MQNLIST** or **GMQNLIST** class with UACC(NONE) specified?	Namelist security should be active, and all profiles *ssid.namelist* should be defined in the **MQNLIST** or **GMQNLIST** class with UACC(NONE) specified.		
95.	Is Read access restricted to those IDs requiring access to make Namelist inquires?	R*ead* access should be to those IDs requiring access to make namelist inquiries.		
	Alternate Userid Security Alternate userid security allows access to be requested under another userid.			
96.	Is Alternate Userid security active and all profiles *ssid.ALTERNATE.USER.alternateuserid* defined in the **MQADMIN** class with UACC(NONE) specified?	Alternate userid security should be active, and all profiles *ssid.ALTERNATE.USER.alternateuserid* should be defined in the **MQADMIN** class with UACC(NONE) specified.		
97.	Is Update access restricted to those IDs requiring	*Update* access t should be restricted to those IDs requiring access to alternate		

Step #	Procedure Description Network Communication	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
	access to alternate IDs?	IDs.		
	Context Security Context security validates whether a userid has authority to pass or set identity and/or origin data for a message.			
98.	Is Context security active and all profiles *ssid.CONTEXT* defined in the **MQADMIN** class with UACC(NONE) specified, where *ssid* is the queue manager name?	Context security should be active, and all profiles *ssid.CONTEXT* should be defined in the **MQADMIN** class with UACC(NONE) specified, where *ssid* is the queue manager name.		
99.	Is *Read* access granted when the PASS option is specified for an MQOPEN or MQPUT1 and is *Update* or *control* access is granted when the SET or OUTPUT option is specified?	*Read* access is required when the PASS option is specified for an MQOPEN or MQPUT1. *Update* or *control* access is required when the SET or OUTPUT option is specified.		
	Command Security Command security validates IDs authorized to issue MQSeries commands.			
100.	Is Command security active and all profiles defined to the MQCMDS class?	Command security should be active, and all profiles should be defined in the **MQCMDS** class.		
101.	Is access to the command security profiles restricted?	Restrict access to command security profiles using the following table:		
	Command	**Profile**		
	ALTER xxxxx	ssid.ALTER.xxxxx		
	ARCHIVE LOG	ssid.ARCHIVE.LOG		
	CLEAR QLOCAL	ssid.CLEAR.QLOCAL		
	DEFINE xxxxx	ssid.DEFINE.xxxxx		
	DELETE xxxxx	ssid.DELETE.xxxxx		
	DISPLAY xxxxx	ssid.DISPLAY.xxxxx		
	PING xxxxx	ssid.PING.xxxxx		
	RECOVER BSDS	ssid.RECOVER.BSDS		
	REFRESH xxxxx	ssid.REFRESH.xxxxx		
	RESET xxxxx	ssid.RESET.xxxxx		
	RESOLVE xxxx	ssid.RESOLVE.xxxxx		
	RESUME QMGR	ssid.RESUME.QMGR		
	RVERIFY SECURITY	ssid.RVERIFY.SECURITY		
	START xxxxx	ssid.START.xxxxx		
	STOP xxxxx	ssid.STOP.CHINIT		
	SUSPEND QMGR	ssid.SUSPEND.QMGR		
	RESLEVEL Security RESLEVEL security profiles control the number of IDs checked for API-resource security.			
102.	Is RESLEVEL security active?	RESLEVEL security should not be implemented due to the following exposures and limitations: 1) RESLEVEL is a powerful option that can cause the bypassing of all security		

Step #	Procedure Description Network Communication	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
		checks. 2) Security audit records are not created when the RESLEVEL profile is utilized. 3) If the WARNING option is specified on a RESLEVEL profile, no warning messages are produced.		
103.	Is a RESLEVEL profile defined for each queue manager and no user or groups specified on the access list?	To protect against any profile in the **MQADMIN** class, such as s*sid.***, resolving to a RESLEVEL profile, a *ssid.RESLEVEL* profile should be defined for each queue manager with UACC(NONE) specified and no users or groups specified in the access list.		
	CICS Transaction Security			
104.	Are MQSeries-supplied CICS transactions properly secured?	MQSeries-supplied CICS transactions should be properly secured.		
105.	Is access to the transactions restricted to CICS regions and the MQSeries administrator?	Access to the following transactions should be restricted to CICS regions and the MQSeries administrator: CKAM CKTI CKQC CKBM CKRT CKCN CKSD CKRS CKDP CKDL CKSQ		
	TOP SECRET			
	Security Classes			
106.	Is Top Secret checking performed on all MQSeries resources?	In order to ensure that TOP SECRET checking is performed on all MQSeries resources, the following RDT entries must exist and be properly owned: MQADMIN MQCONN MQCMDS MQQUEUE MQPROC MQNLIST		
107.	Are the MQSeries subsystem defined?	Define the resources for each MQSeries subsystem to TOP SECRET as follows: TSS ADD(*deptname*) MQADMIN(*ssid*) TSS ADD(*deptname*) MQCONN(*ssid*) TSS ADD(*deptname*) MQCMDS(*ssid*) TSS ADD(*deptname*) MQQUEUE(*ssid*) TSS ADD(*deptname*) MQPROC(*ssid*) TSS ADD(*deptname*) MQNLIST(*ssid*)		
	Started Tasks			
108.	Are started task IDs established for each queue manager started task procedure and distributed queuing started task procedure?	A started task id entry should be created for each queue manager started task procedure and distributed queuing started task procedure.		
109.	Is a corresponding userid	A corresponding userid should be		

Step #	Procedure Description Network Communication	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
	established for each started task?	established for each started task.		
110.	Is the Queue manager and channel initiator started tasks defined without the *BYPASS* attribute?	Queue manager and channel initiator started tasks will not be defined with the *BYPASS* attribute.		
	Datasets			
111.	Are the following data sets APF authorized: *hlqual*.SCSQAUTH *hlqual*.SCSQLINK *hlqual*.SCSQANLx *hlqual*.SCSQSNL *hlqual*.SCSQMVR1 *hlqual*.SCSQMVR2	The installation requires that the following data sets be APF authorized. *hlqual*.SCSQAUTH *hlqual*.SCSQLINK *hlqual*.SCSQANLx *hlqual*.SCSQSNL *hlqual*.SCSQMVR1 *hlqual*.SCSQMVR2		
112.	Is *Read* access to data sets referenced by the CSQINP1, CSQINP2, and CSQXLIB DDs in the queue manager's procedure restricted to the queue manager userid, MQSeries administrator, and systems programming personnel?	*Read* access to data sets referenced by the CSQINP1, CSQINP2, and CSQXLIB DDs in the queue manager's procedure should be restricted to the queue manager userid, MQSeries administrator, and systems programming personnel. Log all access to these data sets.		
113.	Is *Update* access to data set profiles protecting all page sets, logs, bootstrap data sets (BSDS), and data sets referenced by the CSQOUTX and CSQSNAP DDs in the queue manager's procedure restricted to the queue manager userid, MQSeries administrator, and systems programming personnel?	*Update* access to data set profiles protecting all page sets, logs, bootstrap data sets (BSDS), and data sets referenced by the CSQOUTX and CSQSNAP DDs in the queue manager's procedure should be restricted to the queue manager userid, MQSeries administrator, and systems programming personnel. Log all *update* and *alter* access to these data sets.		
114.	Is *Alter* access to all archive data sets in the queue manager's procedure restricted to the queue manager userid, MQSeries administrator, and systems programming personnel?	*Alter* access to all archive data sets in the queue manager's procedure will be restricted to the queue manager userid, MQSeries administrator, and systems programming personnel. Log all *alters* access to these data sets.		
	Connection Security Connection security validates IDs authorized to connect to queue managers.			
115.	Is connection security active and all profiles defined in the **MQCONN** class?	Connection security should be active and all profiles should be defined in the **MQCONN** class.		
116.	Is access to the connection security profiles restricted?	Restrict access to connection security profiles using the following table as a		

Step #	Procedure Description Network Communication	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
		guideline: *ssid*.BATCH - TSO IDs Batch job IDs *ssid*.CICS - CICS region IDs *ssid*.IMS - IMS region IDs *ssid*.CHIN - Channel initiator IDs		
117.	Is access logged by the system?	All access should be logged.		
	Queue Security Queue security validates IDs authorized to access message queues.			
118.	Is Queue security active and all profiles defined in the **MQQUEUE** or **GMQQUEUE** class with UACC(NONE) specified?	Queue security should be active, and all profiles should be defined in the **MQQUEUE** or **GMQQUEUE** class with UACC(NONE) specified.		
119.	Is the Message queue restricted to those IDs that require the ability to get messages from and put messages to message queues?	Message queue access should be restricted to those IDs that require the ability to get messages from and put messages to message queues		
120.	Is access authorization to system queues (those queue resources with a first qualifier of *system*) restricted to the CSQUTIL utility, MQSeries operations and control panels, channel initiators, MQSeries software monitors, and CICS transactions?	Access authorization to system queues (those queue resources with a first qualifier of *system*) should be restricted to the CSQUTIL utility, MQSeries operations and control panels, channel initiators, MQSeries software monitors, and CICS transactions.		
121.	Is an alias queue defined to resolve the real dead-letter queue?	Undeliverable messages can be routed to a dead-letter queue. Two levels of access must be established for these queues. The first level allows applications, as well as some MQSeries objects, to put messages to this queue. The second level restricts the ability to get messages from this queue and protects sensitive data. This should be accomplished by defining an alias queue that resolves to the real dead-letter queue, but defines the alias queue with the attributes **PUT(ENABLED)** and **GET(DISABLED)**.		
122.	Is the ability to get messages from the dead-letter queue restricted to message channel agents (MCAs), CKTI (MQSeries-supplied CICS task initiator), channel initiators utility, and any automated	The ability to get messages from the dead-letter queue should be restricted to message channel agents (MCAs), CKTI (MQSeries-supplied CICS task initiator), channel initiators utility, and any automated application used for dead-letter queue maintenance.		

Step #	Procedure Description Network Communication	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
	application used for dead-letter queue maintenance?			
	Process Security Process security validates IDs authorized to issue MQSeries inquiries on process definitions.			
123.	Is Process security active and all profiles *ssid.processname* defined in the **MQPROC**?	Process security should be active, and all profiles *ssid.processname* should be defined in the **MQPROC** class.		
124.	Is *Read* access restricted to those IDs requiring access to make process inquiries?	Restrict *read* access to those IDs requiring access to make process inquiries.		
	Namelist Security A namelist is a MQSeries object that contains a list of queue names. Namelist security validates IDs authorized to inquire on namelists.			
125.	Is Namelist security active and all profiles s*sid.namelist* defined in the **MQNLIST** class with UACC(NONE) specified?	Namelist security should be active, and all profiles *ssid.namelist* should be defined in the **MQNLIST** class with UACC(NONE) specified.		
126.	Is Read access restricted to those IDs requiring access to make Namelist inquires?	Restrict *read* access to those IDs requiring access to make namelist inquiries.		
	Alternate Userid Security Alternate userid security allows access to be requested under another userid.			
127.	Is Alternate Userid security active and all profiles *ssid.ALTERNATE.USER.alternateuserid* defined in the **MQADMIN** class with UACC(NONE) specified?	Alternate userid security should be active, and all profiles *ssid.ALTERNATE.USER.alternateuserid* should be defined in the **MQADMIN** class.		
128.	Is Update access restricted to those IDs requiring access to alternate IDs?	Restrict *update* access to those IDs requiring access to alternate IDs.		
	Context Security Context security validates whether a userid has authority to pass or set identity and/or origin data for a message.			
129.	Is Context security active and all profiles *ssid.CONTEXT* defined in the **MQADMIN** class, where *ssid* is the queue manager name?	Context security should be active, and all profiles *ssid.CONTEXT* should be defined in the **MQADMIN** class, where *ssid* is the queue manager name.		
130.	Is *Read* access granted when the PASS option is specified for an MQOPEN or MQPUT1 and is *Update* or *control* access is granted when the SET or OUTPUT	*Read* access is required when the PASS option is specified for an MQOPEN or MQPUT1. *Update* or *control* access is required when the SET or OUTPUT option is specified.		

Step #	Procedure Description Network Communication	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
	option is specified?			
	Command Security Command security validates IDs authorized to issue MQSeries commands.			
131.	Is Command security active and all profiles defined to the MQCMDS class?	Command security should be active, and all profiles should be defined in the **MQCMDS** class.		
132.	Is access to the command security profiles restricted?	Restrict access to command security profiles using the following table:		
	Command	**Profile**		
	ALTER xxxxx	ssid.ALTER.xxxxx		
	ARCHIVE LOG	ssid.ARCHIVE.LOG		
	CLEAR QLOCAL	ssid.CLEAR.QLOCAL		
	DEFINE xxxxx	ssid.DEFINE.xxxxx		
	DELETE xxxxx	ssid.DELETE.xxxxx		
	DISPLAY xxxxx	ssid.DISPLAY.xxxxx		
	PING xxxxx	ssid.PING.xxxxx		
	RECOVER BSDS	ssid.RECOVER.BSDS		
	REFRESH xxxxx	ssid.REFRESH.xxxxx		
	RESET xxxxx	ssid.RESET.xxxxx		
	RESOLVE xxxx	ssid.RESOLVE.xxxxx		
	RESUME QMGR	ssid.RESUME.QMGR		
	RVERIFY SECURITY	ssid.RVERIFY.SECURITY		
	START xxxxx	ssid.START.xxxxx		
	STOP xxxxx	ssid.STOP.CHINIT		
	SUSPEND QMGR	ssid.SUSPEND.QMGR		
	RESLEVEL Security RESLEVEL security profiles control the number of IDs checked for API-resource security.			
133.	Is RESLEVEL security active?	RESLEVEL security should not be implemented due to the following exposures and limitations: (1) RESLEVEL is a powerful option that can cause the bypassing of all security checks. (2) Security audit records are not created when the RESLEVEL profile is utilized. (3) If the WARNING option is specified on a RESLEVEL profile, no warning messages are produced.		
134.	Is a RESLEVEL profile defined for each queue manager and no user or groups specified on the access list?	To protect against any profile in the **MQADMIN** class, such as s*sid.***, resolving to a RESLEVEL profile, a *ssid.RESLEVEL* profile should be defined for each queue manager with UACC(NONE) specified and no users or groups specified in the access list.		
	CICS Transaction Security			
135.	Are MQSeries-supplied	MQSeries-supplied CICS transactions		

Step #	Procedure Description Network Communication	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
	CICS transactions properly secured?	should be properly secured.		
136.	Is access to the transactions restricted to CICS regions and the MQSeries administrator?	Access to the following transactions should be restricted to CICS regions and the MQSeries administrator: CKAM CKTI CKQC CKBM CKRT CKCN CKSD CKRS CKDP CKDL CKSQ		

Comments:
Action Plan:

Test Number: **7**	SITE:	DATE:	TIME:
Test Name: **JES2**			
Resources Required:	Mainframe Terminal Access		
Personnel Required:	System Programmer / Security Administrator		
Objectives:	Review of JES2 Controls		
Procedure Description: (Summary)	Verify that the JES2 resource controls are configured to meet USDA policies and requirements.		

Detailed Procedures and Results

Step #	Procedure Description JES2	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
1.	Are JES2 internal mechanisms used for security controls?	Use the services of a security software for security control. JES2 internal mechanisms (e.g., initialization statement parameters and installation exits) should not be used for security control.		
2.	Is SMF data being collected for auditing purposes?	Collect SMF data for auditing purposes.		
3.	Are JES2 resources strictly controlled?	JES2 resources should be strictly controlled. Restrict access to those resources necessary for users to accomplish their assigned responsibilities. The resources to be controlled include, but are not limited to, the following:		
		JES-owned data sets, including SPOOL, SPOOL off-load, checkpoint, libraries containing executable code, commands, exit routines, cataloged procedures, and initialization parameters		
		Input devices including local readers, internal readers, NJE readers, RJE remote workstations, SPOOL off-load receivers, and TSO SUBMIT		
		Output devices including local printers, local punching devices, NJE transmissions, RJE remote workstations, and SPOOL off-load devices		
		Data residing on the JES2 SPOOL (SYSIN/SYSOUT data sets) including JES News, SYSLOG and JES2 traces		
		JES2 commands		
		Job Submissions and naming		
		Surrogate User Privileges (The ability to submit work on behalf of another**)**		
		Jobs and SYSOUT transmitted to and from other NJE nodes.		
		Dumps, logs, and traces of JES2 data		

Step #	Procedure Description JES2	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
4.	Is the SYSLOG and trace data secured from unauthorized access and restricted to only authorized personnel?	The SYSLOG and trace data should be secured from unauthorized access and restricted to only authorized personnel. Uncontrolled access could result in a breach in system and data integrity, or a Potential security exposure.		
	IDs for Remote Processing JES2 allows remote batch workstations to submit jobs, control them, and retrieve their output. JES2 refers to these workstations as RJE workstations.			
5.	Is each remote batch workstation assigned a userid defined without segments or access rights except to the appropriate resources?	Define userid **RMT*nnnn*** for each remote batch workstation, where ***nnnn*** is the number on the RMT statement or **$ADD RMT** command. Do not define any profile segments or grant any access rights except as specified in this section.		
6.	Is each NJE node assigned a userid defined without segments or access rights except to the appropriate resources?	Define userid ***nodename*** for each NJE node, where ***nodename*** is the name on the NODE statement or **$ADD APPL** command. Do not define any profile segments or grant any access rights except as specified in this section.		
	Security Controls for Input The **JESINPUT** class is provided by IBM to control the source of submission for jobs. Optionally, ACF2 and TOP SECRET have their own mechanism to control the source for NJE and RJE submitted jobs.			
7.	Are the JESINPUT resources defined properly with a default access of none and access restricted to only authorized personnel?	The following JESINPUT resources should be defined with a default access of none and access should be restricted to only authorized personnel. JESINPUT class INTRDR *nodename* OFF*n*.* OFF*n*.JR OFF*n*.SR R*nnnn*.RD*m* RDR*nn* STCINRDR TSUINRDR		
8.	Is the resource definition generic if all of the resources of the same type has identical access controls?	The resource definition should be generic if all of the resources of the same type has identical access controls (e.g., if all off-load receivers are equivalent). The default access should be *none* except for sources that are permitted to submit jobs for all users. Those sources may be defined as either *none* or *read*.		
	Security Controls for Output Method to protect the JES2 output resources and the minimal protection to be applied			

Step #	Procedure Description JES2	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
9.	Is the JES2.** WRITER class defined with a default access of none?	The following JES2 OUTPUT resources should be defined the following JES2 resource with a default access of *none*: **WRITER class** ***JES2*.****		
10.	Are the JES2 resources defined properly with a default access of none?	Resources in the a security software's respective **WRITER** class should be defined for each of the following output destinations: *JES2*.LOCAL.*devicename* *JES2*.LOCAL.OFF*n*.* *JES2*.LOCAL.OFF*n*.JT *JES2*.LOCAL.OFF*n*.ST *JES2*.LOCAL.PRT*n* *JES2*.LOCAL.PUN*n* *JES2*.NJE.*nodename* *JES2*.RJE.*devicename*		
11.	Is the resource definition generic if all of the resources of the same type have identical access controls?	The resource definition should be generic if all of the resources of the same type have identical access controls (e.g., if all off-load transmitters are equivalent). If all users are permitted to route output to a specific destination, the resource controlling it may be defined with a default access of either *none* or *read.* Otherwise it should be defined with a default access of *none*.		
	JES2 Spool Data Sets			
12.	Is the JESSPOOL resources defined with a default access of none?	The following JES2 Spool data set resources should be defined in the a security software's respective **JESSPOOL** class with a default access of *none*: *localnodeid*.** *localnodeid*.*JES2*.$TRCLOG.*taskid*.*.JES TRACE *localnodeid*.+MASTER+.SYSLOG.*jobid*.*. SYSLOG		
13.	Are the JES2 resources defined properly with a default access of none?	Define the following resource in the **JESSPOOL** class with a default access of *read*: *localnodeid*.*jesid*.$JESNEWS.*taskid*.D*new slvl*.JESNEWS		
14.	Is the resource definition generic if all of the resources of the same type have identical access controls?	Define a resource in the **OPERCMDS** class for ***JES2*.UPDATE.JESNWS** with a default access of *none*. Permit *control* access for those users responsible for maintaining the JES News data set. All access should be logged.		

Step #	Procedure Description JES2	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
15.	By default does a user have access only to the user's own jobs? Have amendments been made to the standard defaults and have they been documented and approved? Are user's accesses to other jobs documented and approved?	By default a user will have access only to that user's own jobs. However, situations exist where one user legitimately requires access to jobs that run under another user's userid. In particular, if a user routes SYSOUT to an external writer, the external writer must have access to that user's SYSOUT. With the Appropriate approval, the installation may grant a user *read* access to ***localnodeid.userid.jobname.jobid.dsnumber.name*** in the **JESSPOOL** class. All such accesses should be logged.		
16.	Are IDs granted read access to the JES2 trace and SYSLOG data sets if the JES2 trace and SYSLOG data sets are to be transcribed by external writers?	If the JES2 trace and SYSLOG data sets are to be transcribed by external writers, grant the IDs *read* access to the following: *localnodeid*.*JES2*.$TRCLOG.*taskid*.*.JESTRACE *localnodeid*.+MASTER+.SYSLOG.*jobid*.*.SYSLOG This access should be strictly limited to the absolutely minimum number of external writers.		
	JES2 Commands The extended MCS support added in MVS/ESA SP, Version 3, Release 1.3, allows the installation to control the use of JES2 system commands through the a security software. These commands are subject to various types of potential abuse. For this reason, it is necessary to place restrictions on the JES2 system commands that can be entered by particular operators. Some commands are particularly dangerous and should only be used when all less drastic options have been exhausted. Misuse of these commands can create a situation in which the only recovery is an IPL. These commands should be referred to as **sensitive commands**			
17.	Are there user categories defined for the appropriate access to the JES2 resources?	Categories of users should be defined for the following: Network personnel Operations personnel (Junior) Operations personnel (Senior) Systems personnel Users without the above responsibilities Where one of the above includes users with significantly different responsibilities, define as many categories as necessary to give appropriate access to resources at the category level.		

Step #	Procedure Description JES2	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
18.	Are there written policies and procedures for the use of sensitive JES2 commands?	There should be written policies and procedures for the use of sensitive JES2 commands.		
19.	Is access to JES2 commands restricted to the minimum number of personnel, and all access logged?	Access to the JES2 commands should be restricted a minimum number of authorized personnel, and all access logged on the system?		
20.	Is SMF data collected for specific JES2 commands?	SMF data should be collected for specific commands with the exception of DISPLAY.		
21.	Is the JES2.** resource defined in the OPERCMDS with a default access of none?	The *JES2*.** resource should be in the OPERCMDS class with a default access of *none*.		
	Job Submission, Naming, and Control Define and protect the JOB control resources			
22.	Are the JES2 resources defined in the **JESJOBS** class with a default accesses of none?	Define the following with a default access of *none*: **JESJOBS class** **CANCEL.*** **SUBMIT.**** Permit *alter* access to **CANCEL.*localnodeid.userid.jobname*** for those users allowed to cancel the job, and *read* access to **SUBMIT.*localnodeid.jobname.userid*** for those users allowed to submit the job. Use generic profiles (wild cards) as much as possible for this purpose. The permissions granted will take into account installation conventions for job names.		
	Security Controls for Surrogate Users			
23.	Is surrogate permission granted to the minimum number of personnel required for running production jobs?	Allowing a user to be a surrogate for another user gives the user indirect access to the resources available to the execution user. For this reason, grant surrogate permission to the minimum number of personnel required for running production jobs.		

Step #	Procedure Description JES2	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
24.	Are the appropriate SURROGAT resources defined for surrogate job submissions?	Define a resource ***executionuserid*.SUBMIT** in the **SURROGAT** class for each user ***executionuserid*** on behalf of which a surrogate will submit jobs. The default access should be *none*, and logging should be required. Grant *read* access to ***executionuserid*.SUBMIT** for each surrogate user.		
	Remote Processing NJE profiles in the security software's **FACILITY** class are used for command and userid authorization from the network. NJE nodes do not sign on as RJE workstations do, but rather perform the FACILITY/USERID verification as each command is issued.			
25.	Are RJE profiles in the FACILITY class used to force an RJE workstation to log on using a userid and password?	RJE profiles in the **FACILITY** class should be used to force an RJE workstation to log on using a userid (the RJE workstation name) and password using the security software to perform the validation.		
26.	Do profiles in the NODES class control how the security software validates inbound work on an NJE network?	Profiles in the **NODES** class should control how the security software validates inbound work on an NJE network.		
27.	Does the security software commands replace the JES2 commands?	The security software password protection replaces JES2 password protection for remote workstations (specifying RJE passwords in the JES2 startup parameter file).		
28.	Are the appropriate resources defined for remote processing?	Define the following with a default access of *none*: **FACILITY class** **NJE.*** **RJE.*** **NODES class** ***node*.******		
	Enable the security software control of NJE nodes and RJE Workstations			
29.	Are unique userid/user profiles created for each remote workstation or NJE node?	For each remote workstation or NJE node, a unique userid/user profile should be created.		

Step #	Procedure Description JES2	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
30.	Is a profile created in the FACILITY class for each RJE workstation?	For each RJE workstation for which the security software is to check the logon password, create a profile in the security software's **FACILITY** class: ***RJE.workstation*** where ***workstation*** is the RJE workstation ID as defined to JES2 ***NOTE:*** *The mere existence of a profile in the security software's* ***FACILITY*** *class for a remote workstation forces the workstation password to be checked by the security software, rather than by JES2. The specification of access rules has no effect.*		
31.	Is a profile created in the FACILITY class for each NJE node?	For each NJE node for which the security software is to check the command authorization, create a profile in the security software's **FACILITY** class as follows: ***NJE.nodename*** where ***nodename*** is the NJE nodename as defined to JES2		
32.	Is the NODES class established properly?	Define profiles in the security software's **NODES** class in accordance with installation policy. A **NODES** profile name has the following format: ***nodeid.keyword.name***		

Comments:
Action Plan:

Test Number: **8**	SITE:	DATE:	TIME:
Test Name: **SESSION MANAGERS**			
Resources Required:	Mainframe Terminal Access		
Personnel Required:	Systems Programmer / Security Administrator		
Objectives:	Review of Session Manager Standards		
Procedure Description: (Summary)	Verify that the Session Manager resource controls are configured to meet USDA policies and requirements.		

Detailed Procedures and Results

Step #	Procedure Description SESSION MANAGERS	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
	A Session Manager's function is to secure access to both the network and applications running inside the network. It can also act as a front-end security system for the network. ***Examples***: CL/Gateway, Netmaster, TPX, Teleview, IBM's Netview Access Services			
1.	Does the Session Manager interface with the security software via the SAF or equivalent interface to perform security I&A validation?	The Session Manager should interface with the system security software (e.g., ACF2, RACF, TOP SECRET) via the SAF or equivalent interface to perform security I&A validation.		
2.	Are the users validated by the security software and not the Session Manager's internal security control feature?	Only valid users identified to the security software should be granted access to the network, and access to logon to applications in the network. Security information registered within the Session Manager's own internal security control feature will not be used for I&A validation.		
3.	Does Session Manager menus restrict each individual's user's access to only the application each user is authorized to use as defined in the user's security profile?	The Session Manager should restrict each individual user's access only to the applications each user is authorized to use as defined in the user's security profile. Only those authorized applications should be displayed to the user.		
4.	Are SMF records generated for the Session Manager in order to provide audit trails and accounting reports relative to user logon/logoff activity?	The Session Manager will generate SMF records that will then be used to provide audit trails and accounting reports relative to user logon/logoff activity.		

Step #	Procedure Description SESSION MANAGERS	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
5.	Does the Session Manager display a legal notification banner to the user according to the USDA requirements?	The Session Manager will display a legal notification banner to the user according to the USDA requirements.		
6.	Does the Session Manager session successfully terminates applications after the user logs off?	The Session Manager session should successfully terminate applications after the user logs off.		

Comments:
Action Plan:

Test Number: **9**	SITE:	DATE:	TIME:
Test Name**: TERMINAL MONITOR PROGRAMS**			
Resources Required:	Mainframe Terminal Access		
Personnel Required:	Systems Programmer / Security Administrator		
Objectives:	Review of Terminal Monitor Programs.		
Procedure Description: (Summary)	Verify that the Terminal Monitor Programs resource controls are configured to meet USDA policies and requirements.		

Detailed Procedures and Results

Step #	Procedure Description TERMINAL MONITOR PROGRAMS	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
	Terminal monitor programs (TMPs) provide users with a program development system capable of access and manipulating data residing under the controls of the operating system. Some TMP products create an individual address space for each authorized user signing on. However, if the TMP is a multi-user single address space system(MUSASS), all authorized users share the same address space region. Terminal Monitor Programs are products that execute as an interactive online system or run in a batch environment. **Examples:** TSO, CA-Roscoe, some MUSASS [Multi user single address space system]			
1.	Is access to software products data sets controlled and restricted to authorized personnel?	Access to the software product's data sets should be controlled and restricted to authorized personnel.		
2.	Do all TMP systems perform I&A checking during the logon process?	All TMP systems in use at USDA should perform I&A checking during the logon process. Perform I&A validation using the services of the security software.		
3.	Are logon procedures, programs, or profiles assigned to users strictly controlled?	Strictly control logon procedures, programs, or profiles assigned to users. Restrict permission to modify and change user logon assignments only to authorized personnel.		
4.	Is access to data sets specified in logon procedures (e.g., panel libraries, **clist** libraries, etc.) strictly controlled?	Strictly control access to data sets specified in logon procedures (e.g., panel libraries, **clist** libraries, etc.). Only grant the required level of access to users. Restrict *modify/change* access to those individuals responsible for the maintenance of the product or application with which the library is associated.		

Step #	Procedure Description TERMINAL MONITOR PROGRAMS	Expected Results	Actual Results (If different from Expected)	Does Value Match Expected Results? Y/N/P
5.	If TMP products execute as a MUSASS, does the product's internal security provides data integrity and protection?	In TMP products that execute as a MUSASS, the product's internal security should provide data integrity and protection, if it does not compromise the security software security controls.		
6.	Is user access to commands, programs, and facilities within a TMP session restricted?	Restrict user access to commands, programs, and facilities within a TMP session to that necessary for users to accomplish their assigned responsibilities.		
7.	Are product and vendor interfaces reviewed for potential security exposures?	Review product and other vendor interfaces for potential security exposures. Document any potential security exposures.		

Comments:
Action Plan: